Rebuy srl
V.00_june 7 2024

Data Information Security Policy

ANTONELLO DIONISI
Data protection Officer

REBYU SRL
Data Controller

Revision no. 0	Document	Approver Names
Date 07-06-2024	**ISP - INFORMATION SECURITY POLICY**	DPO – IT ADMIN - CEO

PART I

Privacy Policy di **www.rebyu.ai/**

Dati Personali trattati per le seguenti finalità e utilizzando i seguenti servizi:

Contattare l'Utente

Modulo di contatto

Dati Personali: cognome; email; nome; numero di telefono; varie tipologie di Dati

Creazione e gestione di questa Applicazione

WordPress (self-hosted)

Dati Personali: cognome; email; nome; username

Gestione dei tag

Google Tag Manager

Dati Personali: Strumenti di Tracciamento

Registrazione ed autenticazione fornite direttamente da questa Applicazione

Registrazione diretta

Dati Personali: cognome; email; nome; numero di telefono; ragione sociale; varie tipologie di Dati

Informazioni di contatto

Titolare del Trattamento dei Dati

REBYU SRL
Via Lima, 7, 00198 Roma
P.IVA: 17635821006
Indirizzo email del Titolare: info@rebyu.ai

Compliance with the Google Limited Use Policy

Remind to: Google API Services User Data Policy

Google API Services User Data Policy, including the Limited Use requirements.

Rebyu's use of information received from Google APIs will adhere to Google API Services User Data Policy, including the Limited Use requirements.

Limited Use
Our app strictly complies with all conditions specified in the limited use policy of Google.
Do not allow humans to read the user's data unless you have obtained the user's affirmative agreement to view specific messages, files, or other data.
Do not use or transfer the data for serving ads, including retargeting, personalized, or interest-based advertising; and
Limit your use of data to providing or improving user-facing features that are prominent in the requesting application's user interface. All other uses of the data are prohibited;
Only transfer the data to others if necessary to provide or improve user-facing features that are prominent in the requesting application's user interface.

Our privacy policy page documents in detail as following describes what data is requesting and why the requests access to Google user data.

Chapter 1

GENERAL INFORMATION AND FIELD OF APPLICATION

1.1 Introduction

The Information Security Policy (ISP) is the minimum security measure for protecting personal data. The ISP that was contemplated by Italian Presidential Decree 318/99 was completely revised by the EU REG. (ref. GDPR 2016/679).

Based on the new Code:

- The ISP minimum measures must now be adopted by the Data Controller of sensitive or judicial data, conducted by electronic means, and not by an entity, office or natural person legally entitled to do so based on corporate regulations or by the relevant public administration (ref. GDPR 2016/679).
- The ISP must be prepared by parties that previously were required to do so (for example, by whoever processed sensitive or judicial data, but using computers that were not accessible via a telecommunications network available to the public).
- Contrary to the past, the category of judicial data is currently also represented by personal data, referring for example to non-definitive court orders or simply to the capacity as the accused or party subject to investigation (ref. GDPR 2016/679)
- The content of the ISP itself has been supplemented by new features that have been added to those required by previous regulations, or that clarify certain aspects. For example, the ISP now needs to describe the criteria and methods for restoring the availability of data in the event of the information or electronic means being destroyed or damaged; criteria also need to be identified that will be adopted to encode or separate data that can disclose a person's health status and sexual orientation when processed by health authorities and health care practitioners (ref. GDPR 2016/679).

1.2 Field of application

Whoever processes sensitive and judicial data using electronic computers must draw up a Security Policy Document.
The Information Security Policy refers to the processing of all personal data:

- Sensitive data;
- Judicial data;
- Common data.

The Information Security Policy is applied to the processing of all personal data, by:

- electronic processing means;
- Other processing tools (for example, hard-copies, audio, visual and audiovisual, etc.).

The Information Security Policy must be known to and applied by all function comprising the organisation.

1.3 Definitions

Processing
Any operation or series of operations carried out even without the support of electronic tools, relating to the collection, recording, organisation, storage, consulting, processing, amendment, selection, extraction, comparison, use, interconnection, blocking, dissemination, cancellation and destruction of data, even when the latter is not recorded in databases.

Personal data
Any information relating to natural or legal persons, bodies or associations that are or can be identified, even indirectly, by reference to any other information including a personal identification number.

Sensitive data
Personal data allowing the disclosure of racial or ethnic origin, religious, philosophical or other beliefs, political opinions, membership of parties, trade unions, associations or organizations of a religious, philosophical, political or trade-union character, as well as personal data disclosing health status and sexual orientation.

Judicial data
Personal data disclosing the measures referred to in Section 3(1), letters a) to o) and r) to u), of Italian Presidential Decree No. 313 of 14 November 2002 concerning the criminal records office, the register of offence-related administrative sanctions and the relevant current charges, or the status of being either a defendant or the subject of investigations pursuant to Sections 60 and 61 of the Criminal Procedural Code.

Data Controller
Any natural or legal person, government or any other body, association or entity that is competent, also jointly with another Data Controller in determining the purposes and methods of the processing of personal data and the relevant means, including security matters.

Data Processor

Any natural or legal person, public administration, body, association or other agency that processes personal data on the Data Controller's behalf.

Persons in charge of the processing

The natural persons that have been authorised by the Data Controller or Processor to carry out processing operations.

Data subject

Any natural or legal person, body or association that is the subject of the personal data.

Communication

Disclosing personal data to one or more specific parties other than the data subject, the Data Controller's representative in the country, the Data processor and persons in charge of the processing, in any form whatsoever, including by making available or consulting such data.

Dissemination

Disclosing personal data to unidentified persons or entities, in any form whatsoever, including by making available or interrogating such data.

Anonymous data

Any data that either in origin or on account of it having been processed cannot be associated with any identified or identifiable data subject.

Blocking

Retaining personal data by temporarily suspending any other processing operation.

Database

Any organised set of personal data, divided into one or more units located in one or more places.

Electronic communication

Any information exchanged or transmitted between a finite number of parties by means of a publicly-accessible electronic communication service.

This excludes any information conveyed as part of a broadcasting service to the public over an electronic communication network except to the extent that the information can be related to the identifiable or identified subscriber or user receiving the information.

Minimum measures

Any technical, IT, organisational, logistical and procedural security measures comprising the minimum protection level required in relation to the risks provided for in terms of article 31.

Electronic means

The computers, computer software and all electronic or automated devices used for performing the processing.

Computerised authentication

The series of electronic tools and procedures that directly or indirectly verify identity.

Authentication credentials

The data and devices held by a person, known to them or unequivocally associated with them, used for computer authentication.

Password

Part of an authentication credential associated with a person and known to this person, comprising a sequence of characters or other data in electronic format.

Authorisation profile

All the information uniquely associated with a person, which enables the data that said person can access to be identified, and the processing they are authorised to be carried out.

Authorisation system

All the tools and procedures enabling access to data and its processing according to the requesting party's authorisation profile.

Chapter 2

ROLES, TASKS AND DESIGNATION OF ENTITIES

2.1 Data Controller

The **Data Controller** is any natural or legal person, public administration, association or other entity that is competent, also jointly with another Data Controller, to determine the purposes and methods of processing of personal data and the relevant means, including security matters.

The Data Controller must ensure and directly guarantee that security measures are adopted in terms of the PERSONAL DATA PROTECTION CODE and the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES aimed at reducing the risk of data destruction, unauthorised access or processing that is not allowed to a minimum, without prior instructions provided in writing.

With regard to the activities conducted, the Data Controller may if deemed appropriate identify, nominate and appoint one or more Data processors that will ensure and guarantee that the security measures are adopted in accordance with the PERSONAL DATA PROTECTION CODE. In the event that the Data Controller does not appoint any Data processor, the former will take on all the relevant responsibilities and functions.

2.3 Persons in charge of managing and maintaining electronic means

2.3.1 Tasks of persons in charge of managing and maintaining electronic means

The person in charge of managing and maintaining electronic means is the natural person, legal person, public administration and any other entity, association or entity that oversees the resources of the operating system of a computer or a databank system.
In respect of the work conducted, it is the responsibility of the Data processor to identify, nominate and appoint in writing, one or more Persons in charge of managing and maintaining electronic means.
It is the task of Persons in charge of managing and maintaining electronic means to:

- Activate the authentication credentials for persons in charge of the processing, on the orders of the Data processor, for all processing done by electronic means.
- Define which policies to adopt to protect systems from computer viruses, and check on how effective these are on at least a six-monthly basis.
- Protect the computers from the risk of intrusions (hackers violating the system).
- Notify the Data Processor should risks be found relating to the security measures referring to personal data.

If the Data processor does not deem it necessary to appoint a Person in charge of managing and maintaining electronic means, the former will take on all the relevant responsibilities and functions.

2.3.2 Designation of persons in charge of managing and maintaining electronic means

The Data processor appoints one or more Persons in charge of managing and maintaining electronic means, who is tasked with overseeing the proper functioning of the computer system and databanks resources.

Even if not expressly required by regulations, it is worthwhile for the Data Processor to appoint one or more Persons in charge of managing and maintaining electronic means, and to specify the computers or databanks they are entrusted with overseeing.
The Data Processor must inform every Person in charge of managing and maintaining electronic means of the responsibilities they have been entrusted in compliance with the provisions of applicable regulations, and specifically whatever is required by the PERSONAL DATA PROTECTION CODE (Italian Legislative Decree no. 196 of 30 June 2003) and by the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES.
The designation of any Person in charge of managing and maintaining electronic means must be done with a letter of designation, and must be countersigned by the former in acceptance.
A copy of this designation letter must be kept by the Data Processor in a safe place.

The Data processor must provide every Person in charge of managing and maintaining electronic means with a copy of all the rules that refer to the security of processing data that are applicable at the time of the designation.
The designation of the Persons in charge of managing and maintaining electronic means is open-ended, and lapses on cancellation or resignation. This designation may be cancelled at any time by the Data processor without notice, and eventually entrusted to another entity.

2.4 Person in charge of keeping copies of credentials

2.4.1 Tasks of Person in charge of keeping copies of credentials

In respect of the work conducted, it is the responsibility of the Person in charge of personal data security to identify, nominate and design in writing, one or more Persons in charge of keeping copies of credentials.

The task of the Person in charge of keeping copies of credentials is to:

- Manage and see to the safekeeping of the data access credentials for the persons in charge of the processing.
- For each person in charge of the processing, prepare an envelope containing the name of the person, with the credential used inside the envelope. Envelopes with credentials must be stored in a locked and protected place. Instruct the persons in charge of the processing regarding the use of passwords, and the characteristics they should have, as well as the procedures to change them independently.
- Cancel all unused credentials in the event that person in charge of the processing loses the right to access personal data.
- Cancel the access credentials for persons in charge of the processing if they have not been used for over 6 (six) months.

If the Person in charge of personal data security does not nominate a person in charge of keeping copies of credentials, the former will take on all the relevant responsibilities and functions.

2.4.2 Designation of Person in charge of keeping copies of credentials

The Person in charge of personal data security appoints one or more persons in charge of keeping copies of credentials, who are tasked with the safekeeping of passwords to access data stored in the data processor system.
The designation of one or more Persons in charge of keeping copies of credentials must be done with a letter of designation, and must be countersigned by the former in acceptance. A copy of this designation letter must be kept by the Person in charge of personal data security in a safe place.
The Person in charge of personal data security must inform every Person in charge of keeping copies of credentials of the responsibilities they have been entrusted in compliance

with the provisions of applicable regulations, and specifically whatever is required by the PERSONAL DATA PROTECTION CODE (Italian Legislative Decree no. 196 of 30 June 2003) and by the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES.

The Person of charge of personal data security must provide each Person in charge of keeping copies of credentials with a copy of all the rules that refer to the security of processing data that are applicable at the time of the designation.

The designation of the Persons in charge of keeping copies of credentials is open-ended, and lapses on cancellation or resignation.

The designation of one or more Persons in charge of keeping copies of credentials may be cancelled at any time by the Person in charge of personal data security without notice, and eventually entrusted to another entity.

2.5 Person in charge of backing-up databanks

2.5.1 Tasks of Person in charge of backing-up databanks

The Person in charge of backing-up databanks is the natural or legal person that is tasked with overseeing the periodic backing-up of the personal databanks managed.
In respect of the work conducted, it is the responsibility of the Data Processor if necessary, to identify, nominate and appoint in writing, one or more Persons in charge of backing-up databanks.
In order to guarantee the integrity of data against the risk of loss or destruction, and with the technical support of the Person in charge of managing and maintaining electronic means, set the intervals within which backing up must be done on the databanks processed.

The criteria must be agreed on with the Person in charge of managing and maintaining the electronic means in relation to the type of potential risk and according to the level of technology used.

In particular, the following specifications must be set for each databank:

- The Type of support to use for the Back-up Copies.
- The number of Back-up Copies to make each time.
- Whether the supports used for the Back-up Copies can be re-used and if so, at what intervals.
- Whether computerised and scheduled procedures are used to make the Back-up Copies.
- The arrangements to check the Back-up Copies.
- The estimated maximum time for information to be retained without the loss or erasure of data.
- The person in charge of the processing that has been assigned the task of making Back-up Copies.

It is the task of the Person in charge of backing-up databanks to:

- Take all the necessary measures to avoid the loss or destruction of data, and arrange for the periodic recovery of these with back-up copies, according to the criteria set by the Data Processor.
- Ensure the quality of the data back-up copies and that they are kept in a suitable and safe place.
- Ensure the data back-up copies are kept in a suitable and safe place with controlled access.
- Arrange to carefully keep the devices used to make the back-ups, preventing unauthorised staff from gaining access.
- Promptly advise the Person in charge of managing and maintaining electronic means of any problems that could arise during the normal back-up operations.

If the Data processor does not deem it necessary to appoint a Person in charge of backing-up databanks, the former will take on all the relevant responsibilities and functions.

2.5.2 Designation of Person in charge of backing-up databanks

The Data processor appoints one or more Persons in charge of backing-up databanks, who is entrusted with periodically backing-up the databanks managed.

Even if not expressly required by regulations, it is worthwhile for the Data Processor to appoint one or more Persons in charge of backing-up databanks, and to specify the computers or databanks they are entrusted with overseeing.

The Data Processor must inform every Person in charge of backing-up databanks of the responsibilities they have been entrusted in compliance with the provisions of applicable regulations, and specifically whatever is required by the PERSONAL DATA PROTECTION CODE (Italian Legislative Decree no. 196 of 30 June 2003) and by the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES.

The designation of Persons in charge of backing-up databanks must be done with a letter of designation, and must be countersigned by the former in acceptance.

A copy of this designation letter must be kept by the Data Processor in a safe place.

The Data Processor must provide every Person in charge of backing-up databanks with a copy of all the rules that refer to the security of processing data that are applicable at the time of the designation.

2.6.2 Designation of the Persons in charge of the processing of personal data

The designation of any Person in charge of the processing personal data must be done by the Data processor with a letter of designation, which specifies the tasks entrusted, and must be countersigned by the former in acknowledgement.

A copy of the signed designation letter must be kept by the Data processor in a safe place.

The Data processor must inform every Person in charge of the processing of personal data of the responsibilities they have been entrusted in compliance with the provisions of applicable regulations, and specifically whatever is required by the PERSONAL DATA PROTECTION CODE (Italian Legislative Decree no. 196 of 30 June 2003) and by the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES.

The Data processor must provide every Person in charge of the processing of personal data with a copy of all the rules that refer to the security of processing data that are applicable at the time of the designation.

The Persons in charge of the processing must receive appropriate and detailed written instructions, even for similar work groups, on the functions they have been entrusted with and the relevant compliances.

The Persons in charge of the processing must be assigned a password and a computerised authentication code.

The Persons in charge of the processing personal data must adopt the necessary precautions to ensure the secrecy of the password and must diligently safeguard the devices that are for the exclusive use of the persons in charge of the processing.

The designation of the Person in charge of the processing of personal data is open-ended, and lapses on cancellation or resignation. This designation may be cancelled at any time by the Data processor without notice, and eventually entrusted to another entity.

If the Data processor does not deem it necessary to appoint a Person in charge of the processing personal data, the former will take on all the relevant responsibilities and functions.

2.7 Change Management Policy

Change Management Process

The primary goal of the Change Management organization is to accomplish changes in the most efficient manner while minimizing the business impact, costs, and risks. All changes within the Company will be documented. To achieve this, the change management process includes:

• ***Formally Request a Change***

All requests for change will be documented within the company's selected technology platform by creating a new change record. The completion of a new request for change will be completed by the Data Processor with input from the Change Requester (Data Controller).

• ***Categorize and Prioritize the Change***

Data Processor will assess the urgency and the impact of the change on the infrastructure, end user productivity, and budget.

• ***Analyze and Justify the Change***

Data Processor works with the Changer Requester to develop specific justification for the change and to identify how the change may impact the infrastructure, business operations, and budget. Data Processor uses this information to further research and develop an extensive risk and impact analysis.

• ***Approve and Schedule the Change***

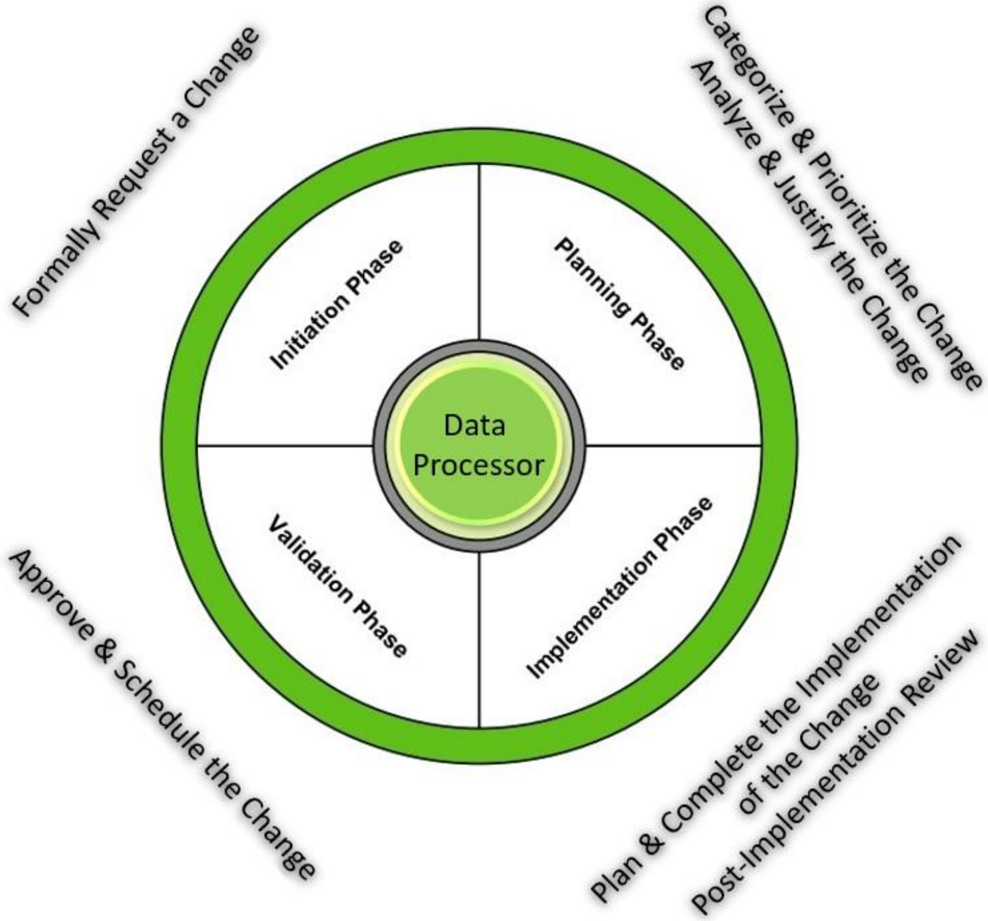
Data Processor uses the company's selected technology platform to record an efficient solution about the Request for Change (RFC), technical and business applications and, in the event of a major or significant change, its approval/rejection.

• ***Plan and Complete the Implementation of the Change***

This process includes developing the technical requirements, reviewing the specific implementation steps and then completing the change in a manner that will minimize impact on the infrastructure and end users.

• *Post-Implementation Review*

A post-implementation review is conducted to ensure whether the change has achieved the desired goals. Post-implementation actions include deciding to accept, modify or back-out the change; contacting the end user to validate success; and finalizing the change documentation within the company's selected technology platform.


Formally Request a Change
Categorize & Prioritize the Change
Analyze & Justify the Change
Initiation Phase
Planning Phase
Data Processor
Validation Phase
Implementation Phase
Approve & Schedule the Change
Plan & Complete the Implementation of the Change
Post-Implementation Review

Chapter 3

PROCESSING WITH ELECTRONIC MEANS

3.1 Computerised authentication system

In addition of new workstation creation or new hire in REBYU structure, it is necessary line up the following suggestions:

Technical Details
Processor Speed up to 2.5 GHz
RAM Size up to 4 GB
Hard Drive Size up to 250 GB
Operating System Windows (Last Released Version)
As a general rule, new workstations has to be able to support efficiently the managed work.

Data Processor must ensure that will be implemented these additional settings
New Windows User
New NAS User
New security credentials
Attended Anti-Virus policies

Therefore, as a general rule values every new hire or into a workstation it has to follow the next guidelines below.

3.1.1 Identification procedure

When processing personal data with electronic means, the Data processor must ensure that processing is only allowed for persons in charge of the processing that have authentication credentials permitting them to follow an authentication procedure for a specific type of processing or a series of types of processing or series of processing.

3.1.2 Identification of person in charge of the processing

The Data processor must ensure that the processing of personal data conducted using electronic means is only allowed to persons in charge of the processing that hold one or more of the following authentication credentials:

- The person in charge of the processing's ID code associated with a reserved password known only to the former
- An authentication device that shall be used and held exclusively by the person in charge of the processing and may be associated with either an ID code or a password
- A biometric feature that relates to the person in charge of the processing and may be associated with either an ID code or a password.

The Data Processor must ensure that the ID code, when used, cannot be assigned to another persons in charge of the processing, not even at a later stage.

The Data Processor must ensure that authentication credentials that are not used for six months are deactivated, unless use is authorised in advance for purely technical reasons.

The Data Processor must ensure that the credentials are also deactivated in the case of loss of quality that allows the person in charge of the processing to access to personal data.

Each Person in charge of the processing be assigned or individually associated with one or more set of authentication credentials.

3.1.3 Characteristics of password

When required by the certification system, **passwords** must consist of at least eight alpha-numeric characters, or if this is not allowed by the electronic means, then by the maximum number of characters allowed.

- The password must not contain references that can easily be traced to the person in charge of the processing.
- Computer equipment, phones, email and internet access are provided for business purposes and monitored regularly to help REBYU defend against cyber-attacks and malicious activity. Limited personal use will usually be acceptable.
- Be vigilant against cyber-attacks and scams such as phishing and report immediately any incidents, including potential or actual losses of REBYU information or assets.
- Guard our intellectual property and respect the intellectual property rights of others.
  - Each desktop needs to adhere to password complexity standards.
  - Passwords will not be shared
  - Enforce Password History: 12 passwords remembered
  - Min password length: 8 characters
  - Password must meet complexity requirements
  - Store passwords using reversible encryption
  - Account Lockout threshold: 6 invalid logon attempts
  - All computerized devices to lock the user interface after no more than 5 minutes.
- The employee has to change proper password when first used, and subsequently user passwords changed every 30 days
- In the case of processing sensitive and judicial data, Admin passwords will be changed every 30
- For each applicable system the re-authentication is required when restoring access to a device interface.
- The person in charge after the change from the product’s default value immediately after installation assures himself and control the password function management process or tool

3.1.4 Precautions to ensure the secrecy of the credential's reserved component

The persons in charge of the processing must adopt the necessary precautions to ensure the password's secrecy and diligently safeguard any other device that they have been entrusted with for the computerised authentication systems (magnetic badges, magnetic cards, etc.).

Mechanisms in place to lock the user interface of a device (workstation, laptop) after no more than 30 minutes of inactivity.

In particular, it is strictly forbidden to communicate one's own access credentials to the IT system to any other person in charge of the processing.

Create and review on an annual basis policy/standard that defines what controls should be in place to secure the company desktops, laptops, mobile device, etc. Workstations and devices used to store (spreadsheets), process or transmit (e-mail) information must be secured as follows:

3.1.5 Instructions for not leaving electronic means unattended and accessible

Persons in charge of the processing are obliged:

- Not to leave their work station unattended.
- Workstations and devices must be locked and/or logged off when unattended.
- Physically secured the device when not in use, cable lock or close under key the room.
- Lock workstations and devices with password request. [See above 3.1.3].

- Close all open applications or better still, switch off the IT system in the case of an extended absence.
- Every workstation has to be set to ask for the password after 5 minutes of inactivity.

3.1.6 Extraordinary access

The persons in charge of keeping copies of credentials are responsible for ensuring that data and electronic means are available in the event of the extended absence or impediment of the persons in charge of the processing, making it crucial and unavoidable to intervene for the sole purpose of maintaining the system's security operational.

The safekeeping of the credential copies is organised so as to guarantee their secrecy.

The persons in charge of keeping copies of credentials must promptly inform the persons in charge of the processing every time that this type of intervention is carried out.

The provisions relating to the authentication system referred to above and those regarding the authorisation system do not apply to the processing of personal data intended for dissemination.

3.1.7 Measures to keeping safety devices

The Data Processor is the person in charge of the processing must ensure that

- All users must use a unique ID to access Attuitude systems and applications. Passwords must be set in accordance with the Password Policy.

- Alternative authentication mechanisms that do not rely on a unique ID and password must be formally approved.

- Remote access to REBYU systems and applications must use two-factor authentication where possible.

- System and application sessions must automatically lock after 15 minutes of inactivity.

3.1.8 Identity and Access

• Uniqueness—Each identifier is unique; that is, eachidentifier is associated with a single person or other entity.
• One Identifier per Individual—An individual may have no more than one REBYU identification number
• Non-Reassignment—Once an identifier is assigned to a particular person it is always associated with that person. It is never subsequently reassigned to identify another person or entity.

To ensure that passwords are of adequate strength, passwords for users, systems, applications, and
devices must meet, to the degree technically feasible, all the Information Security Policy keeping safe necessary requirements.

3.2 Authorisation system

Data processors are tasked with identifying the persons in charge of the processing for each type of personal data databank processed.
Only authorized company desktops/laptops can process AXP data.
The type of processing conducted by each individual person in charge of the processing may differ.
Specifically, the Data processor may afford each person in charge of the processing the possibility of:

- Entering new data into the personal data databank
- Accessing data in display and print mode
- Changing existing data in the personal data databank
- Eliminating existing data in the personal data databank

3.2.1 Cryptography and IT environment structure

The corporate IT structure is essentially composed of the following equipment:

- NAS Server [after called simply SERVER] with AES 256 bit Standard Encryption
- Personal Computer
- Internet devices

NAS is a type of dedicated file storage device that provides local-area network local area network nodes with file-based shared storage through a standard Ethernet connection.
The Advanced Encryption Standard (AES), is a specification for the encryption of electronic data established by the U.S. National Institute of Standards and Technology (NIST) in 2001.
REBYU uses NAS as a Server function to safe, encrypt data and information considered data at rest, separate all data environment how necessary.
Production environment, where software and other products are actually put into

operation for their intended uses by end users, is set on every Processing system.
Non- Production environment is set and encrypted into NAS.
The Processing system and NAS users are produced, authorized and reviewed by Data Processor on an annual basis. HR department send a list of active employee at the beginning of the year and every time occur a change to permit Data Processor checking the active users and remove them when it's necessary.
Non-production environment data cannot stored on production environment and as a general rule every data cannot been stored on non-company owned desktops, laptops and mobile devices because are encrypted into NAS.
Transmission data is done through Voltage Security.
Voltage protects our data as it is used across its entire life-cycle, seamlessly delivering the required levels of protection and enabling safe using data.

3.2.2 Authorisation system: procedure for handling changes.

The entire IT structure should be managed according to the following procedures:

- DbNet S.r.l.will be responsible for management of the hardware and software component and for checking that the configuration and servicing procedures are carried out in full compliance with IT security and privacy regulations.
- DbNet S.r.l.is thus appointed to perform maintenance of the equipment as regards the hardware and software component, and therefore in the case of updating the OS or replacing any hardware component it must duly inform the Data Processor, MAURIZIO DI DOMENICO, of the relative requirements.

PROCEDURES FOR VARIATION AND VALIDATING THE MAINTENANCE OF SECURITY STANDARDS:

- DbNet S.r.l.is bound to adopt the following procedure for any variation or requirement.
  Prepare the relative document composed of and containing the following:
  - Motivation for the request, clearly specifying the need for the work and therefore differentiating between the need for improved performance and updates needed to maintain security standards.
  - The documentation should provide a detailed description of the work to be performed as well as a timeline.
  - Feedback on tests performed on the equipment or similar systems should be included.
  - Whenever, VERISYS S.r.l., will provide due comments on the maintenance of security standards to the Data Controller, including during and after the work.
- The Data Controller will have a team of consultants who will check and authorise such works and which should be composed as follows:
  - The team of consultants, which should never be less than 3 in number, may consist of freelance professionals or persons belonging to companies appointed to the task; separate companies proven not to be related to each other, the applicant (REBYU srl) and the system administrators VERISYS S.r.l..
  - The choice should be made from candidates with proven, specific experience and therefore having the relative certification in their area of expertise.

- In the event of authorisation, the Data Controller will notify the system administrator its consent.
- DbNet S.r.l.will agree to when the works will be carried out, giving due notice to all web users.
- At the end of the works the events/intervention register should be filled in.

The following systems/applications are used for the maintenance, authorisation and tracking of operations performed by each individual operator, specifically:

- Internet access
  - The NAS Server controls who and what may access the internet.
- Encrypted used: **Standard Encrypted AES 256 bit**
- Data Security platform: **NAS Server with Standard Encrypted AES 256**

3.3 Other security measures

Taking into account the provisions of the PERSONAL DATA PROTECTION CODE (Italian Legislative Decree no. 196 of 30 June 2003) and by the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES, it is forbidden for anyone to:

- Make copies on magnetic supports or transmissions not authorised by the Data processor.
- Make copies not authorised by the Data processor, of printouts, schedules, lists, listings and any other materials relating to the personal data to be protected.
- Remove, eliminate or destroy without the authorisation of the Data processor, printouts, schedules, lists, listings and any other materials relating to the personal data to be protected.
- Deliver to people unauthorised by the Data processor, printouts, schedules, lists, listings and any other materials relating to the personal data to be protected.

3.4 Intervals for reviewing the Security Policy Document

By the 31 December 2005 and the 31 March of each year starting from 2006, the Data Controller for sensitive and judicial data must check and possibly draft a revision of the Information Security Policy containing appropriate information relating to points 19.1, 19.2, 19.3, 19.4, 19.5, 19.6, 19.7, 19.8 of the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES OF THE PERSONAL PROTECTION CODE (Italian Legislative Decree no. 196 of 30 June 2003).

3.5 List of the personal data processed

3.5.1 List of the premises and offices where data is processed

The Data processor is responsible for drawing up and updating any changes to the list where data processing is conducted.

3.5.2 List of data archives subject to processing

The Data processor is responsible for drawing up and updating any changes to the list of the types of data processing conducted.
Each databank or archive must be classified according to the data it contains, specifying whether this refers to:

- Common personal data
- Sensitive personal data
- Judicial personal data

3.5.3 List of computer systems for processing

The Data processor is responsible for drawing up and updating any changes to the list of the computer systems used for the data processing.

The following must be specified for each system:

- The person in charge of managing and maintaining the system
- The name of the person/s in charge of the processing using the system

The list of systems that must be kept by the Data processor in a safe place, with a controlled copy sent to the Person in charge of managing and maintaining the relevant electronic means.

3.5.4 List of entities authorised for data processing

The Data processor is responsible for assigning authentication credentials and updating the list of staff authorised to carry out data processing, which must be kept in a safe place, with a controlled copy sent to the Person in charge of keeping copies of the credentials.

3.5.5 Periodic checks on the conditions for maintaining authorisations

By the 31 December of each year, the Data processor is responsible for checking the authentication credentials and updating the list of staff authorised to carry out data processing, which must be kept in a safe place, with a controlled copy sent to the relevant Person in charge of keeping copies of the credentials.

3.6 Analysis of the risks incumbent to the data

3.6.1 Maintenance of data processing systems - Hardware risks

By also making use of internal and external consultants, the person in charge of managing maintenance of electronic devices must check every year on:

- The situation relating to the installed hardware equipment used to process data

- The situation relating to peripheral equipment
- The situation relating to devices connecting to public networks

The purpose is to check the system's reliability, taking into account technological developments in respect of:

- The security of the data processed.
- The risk of loss or destruction.
- The risk of unauthorised access or access that is not allowed

In the event that obvious risks exist, the person in charge of managing maintenance of electronic devices must inform the Data processor so that the necessary measures can be taken to ensure the correct processing of data in compliance with applicable regulations.

3.6.2 Maintenance of operating systems - Software risks

Every year, the person in charge of managing maintenance of electronic devices is responsible for checking the operating systems and software applications installed on the equipment carrying out the data processing.

The purpose is to check the operating system and software application's reliability in respect of:

- The security of the data processed.
- The risk of loss or destruction.
- The risk of unauthorised access or access that is not allowed.

Specifically, taking into account:

- The availability of new improved versions of the software used.
- Patch, Fix or System-Pack reports to remove errors or malfunctions.
- Patch, Fix or System-Pack reports for introducing increased security against the risks of intrusion or damage to data.

In the event that obvious risks exist, the person in charge of managing maintenance of electronic devices must inform the Data Processor so that the necessary measures can be taken to ensure the correct processing of data in compliance with applicable regulations.

3.6.3 Anti-virus policy

As IT Department, Verisys in accordance to Data processor and IT Security Chief.

Purpose

A virus is a piece of potentially malicious programming code that will cause some unexpected or undesirable event. Viruses can be transmitted via e-mail or instant messaging attachments, downloadable Internet files, diskettes, and CD’s. Viruses are usually disguised as something else, and so their presence is not always obvious to the

computer user. A virus infection can be very costly to REBYU in terms of lost data, lost staff productivity, and/or lost reputation.
As a result, one of the goals of REBYU is to provide a computing network that is virus-free. The purpose of this policy is to provide instructions on measures that must be taken by REBYU employees to help achieve effective virus detection and prevention.

Scope

This policy applies to all computers that are connected to the REBYU network via a standard network connection, wireless connection, modem connection, or virtual private network connection.

General Policy

1. Currently, REBYU has Licensed copies of Avira Connect/Avast can be obtained at free online. The most current available version of the anti-virus software package will be taken as the default standard.

2. All computers attached to the REBYU network must have standard, supported anti-virus software installed. This software must be active, be scheduled to perform virus checks real-time scanning, at least weekly scans, log all activity, and apply updates timely at regular intervals, and have its virus definition files kept up to date.

3. Any activities with the intention to create and/or distribute malicious programs onto the REBYU network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) are strictly prohibited.

4. End point protection solution are configured to run at start up and continually protect against malicious activities on desktop, lap and server.

5. If an employee receives what believes to be a virus, or suspects that a computer is infected with a virus, it must be reported to the IT department immediately.

6. No employee should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the IT department.

7. Any virus-infected computer will be removed from the network until it is verified as virus-free.

Rules for Virus Prevention

1. Always run the standard anti-virus software provided by REBYU.

2. Never open any files or macros attached to an e-mail from an unknown, suspicious, or untrustworthy source.

3. Never open any files or macros attached to an e-mail from a known source (even a coworker) if you were not expecting a specific attachment from that source.

4. Be suspicious of e-mail messages containing links to unknown Web sites. It is possible that the link is a malicious executable (.exe) file disguised as a link. Do not click on a link sent to you if you were not expecting a specific link.

5. Never copy, download, or install files from unknown, suspicious, or untrustworthy sources or removable media.

6. If instructed to delete e-mail messages believed to contain a virus, be sure to also delete the message from your Deleted Items or Trash folder.

3.6.3.1 Department and Individual Responsibilities

The following activities are the responsibility of REBYU departments and employees:

1. Departments must ensure that all departmentally - managed computers have virus protection that is in keeping with the standards set out in this policy.

2. Departments that allow employees to use personally - owned computers for business purposes must implement virus protection processes and procedures that are in keeping with the standards set out in this policy.

3. All employees are responsible for taking reasonable measures to protect against virus infection.

4. Employees must not attempt to either alter or disable anti-virus software installed on any computer attached to the REBYU network without the express consent of the IT department.

3.6.3.2 Enforcement

Any employee who is found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

3.7 Measures to adopt to guarantee the integrity and availability of data

In order to guarantee the integrity of data against the risk of loss or destruction, the person in charge of managing and maintaining electronic means sets the intervals within which back-up copies must be made of the databanks processed.
The criteria must be defined according to the type of potential risk and based on the level of technology used.

Instructions for backing-up, checking and recovering data must be provided by the person in charge of managing and maintaining electronic means for each databank. See Annex 9.

The "Document with back-up instructions" must be kept by the Data Processor in a safe place with a controlled copy sent to each person in charge of the back-ups for databanks.

In particular, the following specifications must be set for each databank:

- The Type of support to use for the Back-Up Copies.
- The number of Back-Up Copies to make each time

- Whether the supports used for the Back-Up Copies can be re-used and if so, at what intervals.
- Whether computerised and scheduled procedures are used to make the data Back-Up Copies.
- The arrangements to check the data Back-Up Copies.
- The estimated maximum time for information to be retained without the loss or erasure of data.
- The person in charge of the processing that has been assigned the task of making data Back-Up Copies.
- The instructions and commands needed to make the data back-up copies.
- The instructions and commands needed to recover the data back-up copies.

By the 31 December of each year, the **Data Processor** checks on whether training needs to be periodically provided to staff in charge of processing on the backing up of processed databanks, in relation also to any opportunities offered by advances in technology.

3.8 Procedures for controlling access to the premises where data is processed

The **Data Processor** has the task of drawing up and updating any change to the list of offices where data processing is carried out, and to appoint a person in charge for each office that has the function of directly controlling the systems, equipment or access registers to the premises, with the purpose of preventing intrusions or damage.
The **Data Processor** must define the arrangements for access to the offices housing the systems or access equipment to the data processed.

The **Data Processor** must inform the person in charge of the processing in the office in writing of the tasks they have been entrusted.

3.8.1 Training for the processing of personal data

Based on their experience and knowledge, the **Data Processor** assesses for each person in charge of the processing, and in relation to any opportunities offered by advances in technology, whether it is necessary to plan training sessions on risks incumbent to the data, on the measures available to prevent damaging events, on profiles relating to the protection of the most relevant personal data in relation to the relevant activities, on the resulting responsibilities and on the arrangements for remaining updated on the minimum measures adopted by the Data Controller.
Training is planned from the moment of designation, as well as when someone changes functions, or new tools are introduced that have relevance for the processing of personal data.
By the 31 December of each year, the **Person in charge of personal data security** checks on whether additional training needs to be periodically provided to staff in charge of processing on the backing up of processed databanks.

3.9 Criteria to adopt to ensure that minimum security measures are in place for the processing of personal data, outside of the Data Controller's structure

3.9.1 Processing of personal data outside the Data Controller's structure

The **Person in charge of personal data security** decides whether to entrust the entire or part of the data processing to structures outside the Data Controller.

The Person in charge of personal data security must draw up and update any change to the list of entities carrying out the entirety or partial data processing outside the Data Controller's structure, and for each of these, specify the type of processing conducting, detailing:

- the entities involved
- the place where the data processing physically takes place
- the Data processor for the personal data

The listing of entities that have been entirely or partially entrusted with data processing outside the Data Controller's structure must be kept in a safe place by the **Person in charge of personal data security**. See Annex 8.

In the case where the processing of data is entrusted entirely or partly outside the Data Controller's structure, and it is possible to appoint data processors that can be controlled by the **Data controller** (relating to the arrangements and minimum security measures to adopt for the processing itself), these can be referred to as **Out-sourced Data processors.**

In the case where the processing of data is entrusted entirely or partly outside the Data Controller's structure, and it is not possible to appoint data processors because they are independent entities that cannot be controlled by the Data controller (relating to the arrangements and minimum security measures to adopt for the processing itself), these can be referred to as independent **Out-sourced Data controllers** for the processing, pursuant to Sec. 28 of the PERSONAL DATA PROTECTION CODE. The latter are to be considered independent Data Controllers and therefore subject to the relevant obligations, and are consequently directly and solely liable for any breach of the law.

3.9.2 Criteria for selecting third parties for the outsourced processing of personal data

The **Person in charge of personal data security** decides whether to entrust the entire or part of the data processing to structures outside the Data Controller to entities that have the requirements detailed under Sec. 29 of the PERSONAL DATA PROTECTION CODE (experience, ability and reliability).

The Data Controller that is entrusted with the outsourced processing of data must issue a written declaration stating that suitable security measures have been adopted for the processing in terms of the PERSONAL DATA PROTECTION CODE and the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES.

3.9.3 Designation of the Out-sourced Data processor

For any processing entrusted to an entity outside of the Data Controller's structure, the **person in charge of personal data security** must ensure that security measures are complied with to an extent that is not below what has been set for internal processing.

The designation of the **Out-sourced Data processor** must be countersigned in acceptance, and a copy of the acceptance letter must be kept in a safe place by the Person in charge of personal data security.

The **Person in charge of personal data security** must inform **the Out-sourced Data processor** of the responsibilities they have been assigned in compliance with the provisions of applicable regulations, and specifically whatever is required by the PERSONAL DATA PROTECTION CODE and by the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES.

3.9.4 Designation of the independent Out-sourced Data Controller

For any processing entrusted to an entity outside of the Data Controller's structure, the **person in charge of personal data security** must ensure that security measures are complied with to an extent that is not below what has been set for internal processing.

The designation of the **independent Out-sourced Data Controller** must be countersigned in acceptance, and a copy of the acceptance letter must be kept in a safe place by the Person in charge of personal data security.

The **Person in charge of personal data security** must inform **the independent Out-sourced Data Controller** of the responsibilities they have been assigned in compliance with the provisions of applicable regulations, and specifically whatever is required by the PERSONAL DATA PROTECTION CODE and by the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES.

3.10 Additional measures in the case of processing sensitive or judicial data

3.10.1 Protection against unauthorised access

In order to guarantee the security of sensitive and judicial data against unauthorised access, the **Data Processor** with the support of the **Person in charge of managing and maintaining electronic means**, sets out the technical measures that need to be adopted in relation to the risk of interception, intrusions or hackers on every system linked to a public network.
The criteria must be defined by the **Data Processor** according to the type of potential risk and based on the level of technology used.
In particular, the following specifications must be set for each system:

- The measures applied to prevent intrusions.
- The measures applied to prevent contagion from "computer viruses".

3.10.2 Organisational and technical instructions for safeguarding and using removable supports

The **Data Processor** is responsible for the safeguarding and retention of the supports used to back-up data.

The place where data back-up copies are stored must be identified for each databank, and must be appropriately protected from the potential risks of:

- Chemical agents;
- Heat sources;
- Magnetic fields;
- Intrusions and acts of vandalism;
- Fire;
- Flooding;
- Theft.

Access to the supports used to back-up data is limited for each databank to:

- **The Person in charge of backing-up databanks**
- **The Data processor for the personal data**

3.10.3 Reusing removable supports

Should the **Data processor for personal data** decide that the magnetic supports containing sensitive or judicial data can no longer be used for the purposes they were intended, he/she must arrange for the content to be eliminated, by cancelling and making it unintelligible and ensuring that the data it contained cannot in any way be technically reconstructed.

The Data processor for personal data must ensure that, under no circumstances, copies of databanks containing sensitive or judicial data that are no longer used are left without the content eliminated and cancelled, making it unintelligible, further ensuring that the data recorded cannot in any way be technically reconstructed.

3.10.4 Restoring access to data in the case of damage

The **Data Processor** is exclusively responsible for the decision to restore data availability following its destruction or damage.
The decision to restore data availability must be taken quickly, and in any event, the data availability must be restored at the latest within seven days.
Once the need to restore the availability of data following destruction or damage has been taken, the **Data Processor** must see to the data recovery operation with the **Person in charge of backing-up databanks and the Person in charge of managing and maintaining electronic means**.
The decision to restore the functioning of computers that have broken down is taken exclusively by the **Data Processor**, who can also ask for an opinion from the **Person in charge of managing and maintaining electronic means**. The decision to restore the functioning of broken down computers must be taken quickly, and in any event, the functioning must be restored at the latest within seven days.

3.10.5 Processing done by health authorities and health care professionals

The **Data Processor** must ensure that in the case where there are Databanks containing personal information that could disclose the health status and sexual orientation of a person, the following measures are taken:

- Guarantee that at all times it is impossible for unauthorised access to the data infrastructure and supports.
- Exclude access to persons not authorised for personal data, using an authentication credentials control system.
- If transmitted, the data must be encoded, and the encoding must correspond with a technical level that is adequate for the current status.
- The identification of the relevant user that is entitled to receive data must be unequivocally guaranteed.
- For all Internet services, the security system must be based on a TCP/IP protocol, with Secure Socket Layer (SSL) and 128-bit strong encryption issued by the Verisign Certification Authority, to provide the maximum guarantee that the data transiting on the internet is only visible to the relevant user. Using a 128-bit encryption key ensures the maximum level of security to protect the mutual exchange of data with the relevant user. The time needed to decode this key is virtually infinite (approximately 3 · 1038 possible combinations).
- Architectural separation must be ensured between the machines containing personal data that could disclose health status and sexual orientation, and the servers connected to the Internet.

3.11 Protective measures and safeguards

Policy and standard around Internet Monitoring, Filtering and Usage

To safeguard the IT structure and prevent unauthorized access, unintended modification, disclosure and fraudulent activity of our data, Data Controller has a firewall that filters Malicious and unauthorized websites. Data Processor decides the standards to permit or deny the access to website. As a general rule is not allowed the use of REBYU laptops and workstations for private goals and illegal or dangerous websites such as adult websites, free downloading and similar.
This filter is applied over all PCs net connected.
Monitoring is strictly forbidden by the law attached [LAW MONITORING/FILTERING].

Third-Party Management

The only third party that manages documents containing sensitive data is DHL.
To evaluate the risk assessment we use live monitoring to track the shipments into third party electronic systems.

The steps are:
- Schedule the shipment
- Tracking the detailed shipment content
- Check the track through the waybill
- Courier signature
- On line shipment monitoring
- Verify the shipment arrival

- Checking with shipment tracking

In the case of shipment loss or missing of one step above, the only thing we can do is contacting the authority with relative complain. Then, we aware all people involved with the shipment.

DHL has proper responsibilities according to the terms and conditions of carriage.

3.11.1 Description of interventions carried out by outside entities

Should outside entities be used to see to the proper functioning of hardware and/or software of electronic means, and for any repairs, updates or replacements that may be required, the **Data processor** must duly receive from the staff carrying out the technical intervention, a written declaration with a detailed description of the work done, certifying that this complies with the provisions in the PERSONAL DATA PROTECTION CODE (Italian Legislative Decree no. 196 of 30 June 2003), and with special reference to the provisions under point 25 of the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES.
(See the procedure communicated in the attached letter)

3.11.2 Control procedure for changes to the system

Control procedures for equipment:

- **Data server**

The following procedures must be followed in the case of a Server breakdown.

1) Check that individual Personal Computers cannot actually access the web enabled files, even after switching off and restarting the Personal Computers.
2) Contact one of the Company data processors to report the problem
3) The Company data processor must check the server status; if the server is on, switch off and restart the server.
4) If it functions properly after restarting, report the event in the events and interventions register.
5) Should the problem persist, contact the support service provider, recording the event in the events/interventions register.

Control procedures for technical interventions.

6) Check that before the technician begins any work, the “Events/interventions register” is checked and he/she begins filling it in.
7) In the case of access to the Server, check that the technician has found that the back-up exists.
8) Then in the case of actual access to the back-up data (functioning), check that the data is available offline from the server.
9) At this point, the technician can operate and carry out the recovery/repair to the Server.

Procedures after the recovery.

10) Complete the events/interventions register.
11) In the case of a Hard Disk being replaced, check that the disc is completely cancelled, according to the various options (as per the recommendations of the Data Protection Authority available online at the following address:
http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1574080

In the case of interventions to update and perform maintenance

1) The Company data processor can provide the relevant Technician with a temporary password to access the server.
2) In the case of system updates relating to the operating system and once it has been established that these updates are effectively necessary and are part of the improvements to security released by the manufacture (for example, Microsoft in the case of equipment with the Windows operating system), these can be carried out and installed without further authorisation. Nonetheless:
    a. Before continuing, ensure that the technician has first made a back-up copy with relevant access and functioning tests.
    b. Always record the event in the "Events/interventions register".
3) In the case of various applications being installed, the procedure below should be followed.
    a. The requesting staff as the user must make the relevant request and report the need for and/or existence of updates to the Project Manager.
    b. Subject to checking using various procedures (tests, simulations and/or others) and if the tests are positive, the Project Manager will report the relevant requirement to the Data processor/Administration.
    c. If accepted, the Data processor/Administration will in turn proceed with the request and communicate to the Technical staff to go ahead with the update, and will complete the "Events/interventions register".
    d. During the intervention stage, check that the Technical staff have first made a back-up copy with the relevant access and functioning tests, and completed the "Events/interventions register".

- **Email server**

The following procedures must be followed in the case of a Server breakdown.

1) Check that individual Personal Computers cannot actually access the web enabled files, even after switching off and restarting the Personal Computers.
2) Contact one of the Company data processors to report the problem
3) The Company data processor must check the server status; if the server is on, switch off and restart the server.
4) If it functions properly after restarting, report the event in the events and interventions register.
5) Should the problem persist, contact the support service provider, recording the event in the events/interventions register.

Control procedures for technical interventions.

6) Check that before the technician begins any work, the “Events/interventions register “ is checked and he/she begins filling it in.
7) In the case of access to the Server, check that the technician has found that the back-up exists.
8) Then in the case of actual access to the back-up data (functioning), check that the data is available offline from the server.
9) At this point, the technician can operate and carry out the recovery/repair to the Server.

Procedures after the recovery.

10) Complete the events/interventions register.
11) In the case of a Hard Disk being replaced, check that the disc is completely cancelled, according to the various options (as per the recommendations of the Data Protection Authority available online at the following address: http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1574080

In the case of interventions to update and perform maintenance

1) The Company data processor can provide the relevant Technician with a temporary password to access the server.
2) In the case of system updates relating to the operating system and once it has been established that these updates are effectively necessary and are part of the improvements to security released by the manufacture (for example, Microsoft in the case of equipment with the Windows operating system), these can be carried out and installed without further authorisation. Nonetheless:
    a. before continuing, ensure that the technician has first made a back-up copy with relevant access and functioning tests.
    b. Always record the event in the "Events/interventions register".
3) In the case of various applications being installed, the procedure below should be followed.
    a. The requesting staff as the user must make the relevant request and report the need for and/or existence of updates to the Project Manager.
    b. Subject to checking using various procedures (tests, simulations and/or others) and if the tests are positive, the Project Manager will report the relevant requirement to the Data processor/Administration.
    c. If accepted, the Data processor/Administration will in turn proceed with the request and communicate to the Technical staff to go ahead with the update, and will complete the "Events/interventions register".
    d. During the intervention stage, check that the Technical staff have first made a back-up copy with the relevant access and functioning tests, and completed the "Events/interventions register".

3.11.3 Report for the financial statements

If a Report is required to accompany the Financial Statements, the Data Controller must refer to the Information Security Policy being drafted or updated, certifying compliance with the provisions of the PERSONAL DATA PROTECTION CODE (Italian Legislative Decree no. 196 of 30 June 2003) and by the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES.

3.12 Data Deletion Policy

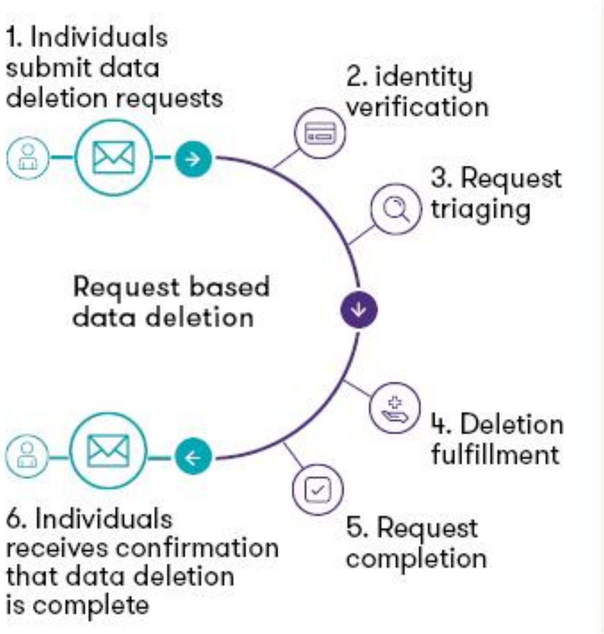
Data Deletion means the physical or technical destruction (or anonymization) sufficient to make the information contained in a document no longer recoverable by ordinary commercially available means.

The Data Controller has adopted agreed and approved destruction methods by IT technicians, which can be used for any type of information stored on electronic/multimedia media such as CD-ROMs, DVDs, USB sticks and other types of mobile media, hard drives, mobile devices , portable drives or registered databases or backup files.

The paper documents will be shredded in a secure way and the relative workstations closed in the office of the appointed person. Waste will be periodically collected only by authorized personnel for disposal.

3.12.1 Automatic Process Data Deletion

In general, there are two types of data deletion required by privacy regulations: request-based deletion and/or data retention and purge.


1. Individuals submit data deletion requests
2. identity verification
3. Request triaging
Request based data deletion
4. Deletion fulfillment
5. Request completion
6. Individuals receives confirmation that data deletion is complete

Data retention schedule and **Data destruction schedule** are two real-time services available for end-to-end automation of personal data removal.
The process collect a log destruction or deletion of the data for verification purposes, especially in cases of data subject requests.

IT process provides a weekly schedule that performs deletion/anonymization of all documents on the list valued according to manual requests and retention rules listed in the table indicated in the next paragraph.

The process produce an output list of deleted/anonymised documents. This list are stored in the register for future reference.
Eventualy non-conformities are reported to the IT office and the persons responsible for the control.

3.12.2 TABLE of Retetion times

Department/Area	Type of tratment	Retetion times	Normative References
CAREER SERVICE	treatment for the management of internship and placement activities	The data will be kept indefinitely but will be used for the purpose subject to processing for a time not exceeding 5 years following the termination of employee status.	Art. 2220 C.C.
BUSINESS PROPOSAL AREA	The data is treated for the realization of the commercial offer for the business proposition	Contract Indication o Expiration	Linee guida CODAU
ACCOUNTING AND FINANCIAL STATEMENT	The data is processed for the performance of activities of an organizational, administrative, financial and accounting nature functional to the fulfilment of obligations contractual and fiscal	10 years	Art. 2220 C.C.
HR	employee data processing the management of the employment relationship (personal data, pay slips, attendance)	No limits	Linee guida CODAU
	processing for training and updating professional	No limits	Linee guida CODAU
	processing aimed at managing the relationship with contract staff	10 years after the termination of the employment relationship	Company Policy
	treatment carried out with Libro Unico del lavoro (LUL)	5 years since last registration	Decreto Ministeriale del 9 luglio 2008 - art. 6, comma 2: in riferimento al LUL prevede un periodo di 5 anni dall'ultima registrazione
	processing of personal data of trainees	10 years after the termination of the employment relationship	Company Policy

3.12.3 Records Destruction Holds

An exception to the usual destruction procedure is made in the case of a Records Destruction Hold. In the case of litigation, an investigation or some other situation, it may be necessary to retain specific records until the issue is resolved. These records may not be transferred or destroyed until notice is given by the proper authorities. Specific instructions about records which must be preserved beyond their usual scheduled retention will be distributed to all employees via e-mail.

Chapter 4

SECURITY PLAN

This chapter contains the security measures adopted for the formation, management, transmission, exchange, access and retention of electronic documents, with reference to the regulations on the protection of personal data.

4.1 Objectives of the security plan

The emergency plan guarantees that:

- In the case of an external attack, all the measures needed to minimise damage are implemented;
- In the case of an internal attack, the causes or those guilty are found and the damage eliminated.

The security plan guarantees that:

- the documents and data processed by the Company are made available, are complete and confidential;
- the common personal data, sensitive and/or judicial data is kept in such a way that it reduces the risk of destruction or loss, even by accident, unauthorised access or processing not permitted or compliant with the purposes it was collected to a minimum, by adopting appropriate and preventative security measures, in relation to the know-how accumulated on the basis of technical progress, their nature and the specific processing characteristics.

4.2 General information

The person in charge of Protocol works in conjunction with the Person in charge of the IT system and the Data Processor and/or other trusted experts to prepare the security plan, pursuant to Sec. 44 of the CAD.

The security plan is based on the results of the analysis of the risks that the data is exposed to (both personal and non-personal), and/or the documents processed and the strategic directives set by REBYU management. The security plan defines:

- the general and specific security policies for the Company to adopt internally;
- the Protocol access procedures;
- the operational interventions undertaken in terms of organisation, procedures and technical aspects with special reference to the minimum security measures pursuant to the technical specifications in Annex b) of Italian Legislative Decree no. 196 of 30 June 2003, the Personal Data Protection Code, in the case of personal data processing;
- the specific training plans for staff;
- the procedures whereby periodic monitoring is done on the effectiveness and efficiency of the security measures.

4.3 Handling the reporting of accidents

It is never possible to predict if and when an external attack may occur, considering that these are made by hackers who target the servers for various reasons.
This is also true of internal attacks. For this reason, the Company has adopted all the devices and software needed to passively prevent this type of attack. This is the passive security of prevention.
To offer protection from these attacks, instead, the company has its own IT Security Chief.
As soon as he identifies the risk of a possible external attack or of an internal incident of any nature, with the help of the passive instruments just mentioned, he raises the alarm to all the customers connected at the time, giving the order to disconnect and turn off the devices, as well as immediately contacting the external server operators and disconnecting the main server inside the Company.

This way, having physically isolated the devices, investigations as to the source of the attack may begin and an estimate of the possible damages or loss of data may be made. For such events please refer to the relevant chapters.
After contacting the company responsible for the maintenance of the server, the problem will be tackled and resolved, restoring the existing defence systems and continuing with company activities.
All employees have received training on the identification of possible problems or incidents and attacks, and are familiar with the necessary procedures.

4.4 Development of electronic documents – security aspects

The instrumental resources and procedures used to develop electronic documents ensure:

- the entity that developed the document and the reference administration can be identified;
- the signing of electronic documents, when required, using a digital signature in accordance with applicable technical regulations;
- the suitability of the documents to be managed by means of electronic instruments and to be recorded;
- access to the electronic documents by means of computerised systems;
- the legibility of the documents over time;
- the inter-changeability of documents;

The electronic documents generated are converted, prior to their being digitally signed into a PDF format, so as to ensure they are legible on other systems, that they cannot be altered during the access and retention stages and that the content and structure of the document do not change over time.

The transmission procedure to the signing of the PDF file referred to above is done via internal electronic
mail. Whenever the entity that needs to sign the document has changes to report, this should always be done by sending an email to the sender.

To ensure the Data Controller and integrity are assigned properly, the document is signed with a digital signature.
To ensure that a definite date is given to an electronic document generated within the Company, the rules on the temporal validation and protection of electronic documents in

accordance with the Decree of the Council of Ministers' President dated 13 January 2004 (technical rules for the formation, transmission, retention, duplication, reproduction and validation - including temporal of electronic documents) are applicable.

4.5 Management of protocol and security recordings

Security recordings are made up of any kind of information (for example, data or transactions) that exist or transit on platforms, which it is worthwhile keeping because they could be needed either in the case of legal disputes referring to the operations carried out on the system, or in order to fully analyse the causes for any security incidents.

Security recordings consist of:

- system logs generated by the operating system;
- the logs of peripheral protection devices on the computer system (Intrusion Detection System (IDS), network sensors and firewalls);

4.6 Access to electronic documents

Access control is guaranteed by using an authorisation system based on the access credentials to one's own computer via Active Directory. User profiling takes place beforehand and makes it possible to define the qualifications/authorisations that can be carried out/released for each single user.

The computer protocol system used:

- allows for the differentiated access control of resources to the system for each user or user group;
- ensures tracking of any amendment event of the data processed and identifying its author. These recordings are protected so that unauthorised changes are not allowed.

Each user can only access the documents that have been directly assigned, or documents sent to their UOR. The Head of a UOR that reports in order of hierarchy to other UORs, can view the documents assigned to these structures.

The system also allows for a different level of confidentiality to be associated with each type of document processed by the administration. Documents are never viewed by users without access rights, not even when a general search is being conducted in the archive.

4.7 Retention of electronic documents

The retention of electronic documents is based on the procedures and technical specifications detailed in CNIPA resolution no. 11 dated 19 February 2004 and subsequent amendments.

4.8 Electronic storage service

The person in charge of the electronic storage of documents sets the provisions to correspond with the general security plan and the guidelines provided by the Head of

Protocol, to ensure that saving operations of data on removable electronic supports are carried out correctly.

The person in charge of digital storage:

- adopts the necessary measures to guarantee the physical and logical security of the system used for the electronic storage process and back-ups of storage supports, by using technology tools and the procedures referred to above;
- ensures that the data acquired in previous versions can be fully recovered and reused, in the case of the storage system being updated;
- defines the content of the storage supports and back-ups;
- periodically and at intervals of not more than five years, checks that the stored documents are effectively legible,
- and if necessary, copies the support content.

Chapter 5

DISASTER RECOVERY PLAN (DRP)

5.1 Purpose of the document

The purpose of the Plan is to ensure full and total recovery of customers' electronic documents subsequent to a disastrous event.

5.2 List of System and Application Procedures

DOCUMENT NAME	Version	Owner
DRP	OO	DPO - IT MANAGER

5.3 Scope of the DRP

The services in question are provided by separate localised infrastructure.

Figure 2 below shows a logical representation of the architectural design offered and implemented. In the green quarter of the circle on the bottom left, reference is made to the DRP solution, with the relevant architectural design shown in Figure 3.

Figure 2 is broken down over three sections:

- on the top, the internet connectivity from/to the outside,
- in the centre, the business logic that provides the services (front-end)
- below, the data management section (or data, or back-end).

XXXXX are customer applications/servers.

As far as the data section (back-end) is concerned, which is positioned on a private network connected to the business logic section via appropriate internet devices, there are Oracle databases on IBM clusters in High Availability (HA), SAN IBM storage apparatus, file server structure and NAS, IBM TSM back-up servers and relevant tape library.

The secondary DRP site is expected to have a structure organised in an equivalent fashion from a logical perspective to what exists at the production site.

There will therefore be three sections: the internet connectivity to the outside, the business logic section that provides the services (front-end) and the data section (back-end) with the relevant internal connectivity.

For the internet connectivity to the outside, 1 Infracom link, two Load Balancers to balance the load towards the farms, and a connectivity section to the network are envisaged.

The business logic section (front-end) will consist of server farms consisting of one or more virtual servers. The virtualisation platform will be based on UCS/VMWARE technology, with Fabric Interconnect apparatus for the connection to the internet and to storage.

For the data management section (back-end), there will be an Oracle database on virtual machines, SAN storage apparatus, file server structure and NAS.

A complete back-up of the databases making up the XXX services will be sent to the secondary DRP
site. The intervals must be compatible with the RPO specified by the SLA set by contract. The

technical operations that will be carried out to restore services and detailed in the plan, mainly consist of:

- server activation/switching on procedures for the business logic section with possible application updates
- start-up/update and testing of DB requests making up the service, via the importing of the latest data
- application testing

The Table shows the responsibility matrix per layer for the DRP solution. Installation and solution operations persons in charge are applicable for all layers.

Layer		Person in charge of installation	Person in charge of operations
Layer 1		tbd	
Layer 2		tbd	
Layer 3		tbd	
Layer 4		tbd	
Layer 5		tbd	
Layer 6		tbd	
Layer 7		tbd	
Layer 8		tbd	
Layer 9		tbd	

Table 4 - Responsibility matrix for the DRP solution

5.4 Plan Activation

Emergency Alert In the event that a situation or disaster occurs at REBYU Srl, **the Person in charge of BRP** is responsible for contacting the competent authorities (Police Dpt.) and assessing the emergency situation. An Alert will be sent to all AXP Department Heads.

Status updates will be provided by the Person in charge of BRP to the AXP Department Heads for dissemination of pertinent information.

The disastrous event communication occurs by detailed email sent to AXP Department Heads waiting for the reply about actions to do.

Chapter 6

BUSINESS CONTINUITY PLAN (BCP)

6.1 Scope and objectives of the BCP document

This document refers to the operations to recover the critical processes of XXXXX Services, identified as such during the BIA, and managed by the following organisational units:

ID	Process	Organisational Unit	Departmental Procedure	CO	Priority to restore
1	System Help Desk				1
2	Application Help Desk				2

Table 1: Organisational units in the BCP context

The processes above must be restored with the objectives set out below:

ID	Critical Process	RTO	RPO
1	System Help Desk		N/A
2	Application Help Desk		N/A

6.2 Responsibilities for process recovery activities

The operational coordination of recovery activities for critical processes is entrusted to the **Person in charge of BRP**, in this case the:

- Person in charge of the **CERT/SOC function**

That in this capacity reports to data processor.

The Person in charge of BRP has the responsibility of coordinating the various functions involved in the recovery process, including those outside of the originating function. [The coordination responsibility is usually assigned on the basis of the role of the processes managed by the organisational unit in relation to the others.]

The basic objective of the coordination is to comply with the RTO/RPO targets assigned.

In the absence of a Person in charge of the **CERT/SOC** function, the role is covered by the:
Deputy

For the recovery of perimeter processes, the **Person in charge of BRP** coordinates the recovery operations conducted by the following organisational units. They are responsible only for the perimeter activities up until these are restored to the **Person in charge of BRP**:

Organisational Unit	Data Processor	Deputy Notes
Technical Office	...	
Team ...		
Department of Reference		

6.3 Alternative premises (Help Desk operational premises). OU placement

The table below shows the human resources used under normal and Emergency conditions for critical processes.

Organisational Unit	Process	Resources under normal conditions	Resources per CO	Office	Notes

6.4 Action Plan of Person in charge of BCP

At the time that crisis status is initiated by the Crisis Committee, the Person in charge of BRP is informed of this by the Person in charge of BCP and/or the Head of the Crisis Committee and proceeds as follows:

1. He/she ensures that they are in secure and protected conditions, from where the actions detailed below can be carried out. The pre-defined secure position, outside the normal offices, is as follows:

    - During working hours: tbd
    - Outside working hours and in progress: own home or motor car

2. A check is made that the staff belonging to the organisational unit are not in danger, for example, still inside the offices that need to be evacuated. In the case of any doubts, contact the **Head of the Crisis Committee** and/or the operations officer of the Crisis Committee to obtain information and instructions.

3. Contact and check with the Person in charge of BCP whether to immediately activate the BRP plan, set priorities and changes to the established Plan on the basis of the characteristics of the current crisis.

4. If the decision is to postpone activating the BCP, the Person in charge of BRP asks for confirmation from the Head of the Crisis Committee to demobilise its staff, and then advises the staff in the organisational unit to return/remain at home. The communication can be made by telephone during working hours or via email/SMS outside of working hours.

5. If the decision is to shortly activate the BCP, and the staff has been evacuated or is outside the usual work place, the Person in charge of BRP will contact the Head of the Crisis Committee to decide whether to keep the staff where they are pending instructions or if they should be moved to a safe area or to different offices or told to go home. The staff is consequently either notified directly or via cell/SMS.

6. The Person in charge of BPR will contact the Heads of the Organisational Units involved and inform them to prepare implementing their Departmental BC Plan and to remain available and in contact until further instructions. The former also checks their position and that they are in a safe position to await new instructions. Otherwise, the CERT is contacted to report on the dangerous conditions.

7. Once confirmation is received to activate the BRP, the Person in charge of BRP will contact the Person in charge of DRP, and will ascertain the status of recovery operations for essential applications to restore critical processes (System and Application Help Desk).

8. The Person in charge of BRP will then contact the Heads of the Organisational Units, and based on the contingent priorities will jointly decide on:

    - The staff that needs to be at alternative premises and when (assess whether to send someone to the DR site).
    - Staff that can operate from home, by remotely accessing the VPN
    - Staff that can remain passive (on leave)

9. The Person in charge of BRP checks the progress status of the support applications and reports the following to the Person in charge of BCP:

    a. Confirms application availability (HD)
    b. Confirms availability of work stations
    c. Necessary actions:
        i. Any requests for services from third parties (suppliers, etc.)
        ii. Any requests for additional staff
        iii. Any requests for specific equipment
    d. Any information to be conveyed to end customers
    e. Estimate on when the recovery operations will be completed and compliance with RTO

10. The Person in charge continues to coordinate recovery operations, coordinating this with the other OU Heads, the Person in charge of DRP, the Head of the Technical Office, until the required service level is reached.

11. The Person in charge of BRP will collect and report any requests (services, staff, purchases, etc.) to the Person in charge of BCP, who will in turn convey these to the Crisis Committee, and be assigned by the Committee to the different Company functions.

12. The Person in charge of BRP confirms with the BCP Head when the recovery operations are completed.

Chapter 7

PROCESSING WITHOUT ELECTRONIC MEANS

7.1 Designation and instructions to persons in charge of the processing

In respect of each archive, Data processors must establish a list of persons in charge of the processing, who are authorised to access them and give instructions directed at ensuring continual control over archive access.
Persons in charge of the processing that deal with deeds and documents containing personal data must retain and return them once the operations are completed.

Should the documents contain sensitive or judicial data pursuant to Sec. 4 of the PERSONAL DATA PROTECTION CODE, the persons in charge of the processing are obliged to retain these until they are returned in locked containers.

Access to archives containing documents that have sensitive or judicial data is allowed after hours, on identification and recording of the entities.

7.2 Copies of deeds and documents

Based on the provisions of the PERSONAL DATA PROTECTION CODE (Italian Legislative Decree no. 196 of 30 June 2003) and by the TECHNICAL SPECIFICATIONS ON MINIMUM SECURITY MEASURES, it is forbidden for anyone to:

- Make photostat or another other type of copies not authorised by the Data Processor, of printouts, schedules, lists, listings and any other materials relating to the personal data that is processed.
- Remove, eliminate or destroy without the authorisation of the Data Processor, printouts, schedules, lists, listings and any other materials relating to the personal data that is processed.
- Provide anyone not authorised by the Data Processor, with printouts, schedules, lists, listings and any other materials relating to the personal data that is processed.

Chapter 8

RIGHTS OF THE DATA SUBJECT

8.1 Right to access personal data

1. The data subject shall have the right to obtain confirmation as to whether or not personal data concerning him/her exists, also if not yet recorded, and communication of such data in an intelligible form.

2. The data subject shall have the right to be informed regarding:

   a. the source of the personal data;
   b. the purposes and methods for processing;
   c. the logic applied to the processing, if this is being carried out with the support of electronic means;
   d. the identification data concerning the data controller, data processors and the representative designated as per article 5, section 2;
   e. the entities or categories of entities to whom or which the data may be communicated, or that may come to know of the data in their capacity as designated representative in the State's territory, data processors or persons in charge of processing;

3. The data subject has the right to obtain:

   a. the updating or correction of the data or, where it is in his interests, the addition of further data;
   b. the deletion, rendering anonymous or blocking of data that has been processed in violation of the law, including data whose retention is unnecessary in relation to the purposes that said data was collected or subsequently processed for;
   c. certification that the operations as per points a) and b) have been made known, also with regard to their content, to those to whom the data have been communicated or disseminated, except when this duty is found to be impossible or entails the use of means manifestly disproportionate to the right to be safeguarded.

4. A data subject shall have the right to object, in whole or in part:

a. on legitimate grounds, to the processing of personal data concerning him/her, even though they are relevant to the purpose of the collection;
b. to the processing of personal data concerning them where this is done for the purposes of sending advertising material or direct selling or for conducting market research or business communications.

8.2 Exercise of rights

1. The rights referred to under Sec. 7 can be exercised in an informal request addressed to the Data Controller or Data Processor, or even forwarded via the persons in charge of the processing, and should receive a timely response.

2. The rights pursuant to Section 7 cannot be exercised in a request to the Data Controller or Data processor in terms of Section 145, if the processing of personal data is done:

   a. in accordance with the provisions of Decree-Law no. 143 of 03 May 1991, converted with amendments by Law no. 197 of 05 July 1991 and subsequent amendments on the issue of money laundering;
   b. in accordance with the provisions of Decree-Law no. 419 of 31 December 1991, converted with amendments by Law no. 172 of 18 February 1992 and subsequent amendments on supporting the victims of extortion demands;
   c. by Parliamentary Committees established in terms of Section 82 of the Constitution;
   d. by a public entity, other than economic public entities, based on a specific provision of the law, for the sole purposes related to monetary and currency policy, payments system, the control of financial brokers and credit and financial markets, as well as the protection of their stability;
   e. in terms of Section 24, paragraph 1, point f), limited to the time period when an effective and material prejudice could result on conducting investigations by defence counsel or exercising rights in court;
   f. by providers of electronic communication services accessible to the public, relating to incoming telephone communications, unless an effective and material prejudice could result on conducting investigations by defence counsel as referred to in Law no. 397 of 07 December 2000;
   g. for reasons of justice, at the judicial offices of any grade and level, or the Superior Magistrate's Council or other self-governing entities or the Ministry of Justice;
   h. Pursuant to Section 53, without prejudice to the provisions under Law no. 121 of 1 April 1981.

3. On being reported by the data subject in the cases referred to under Section 2, paragraphs a), b), d), e) and f), the Data Protection Authority implements this as per sections 157, 158 and 159, and in the cases referred to under points c), g) and h) of the same section, implements this according to section 160.

4. Exercising the rights under Section 7, when this does not relate to objective data can be done, unless this concerns the rectification or addition of evaluative personal data, relating to judgements, opinions or other subjective assessments, including directives on the behaviour to adopt or decisions pending by the Data Controller.

8.3 Exercise procedures

1. The request addressed to the Data Controller or Data processor can be sent by registered letter, fax or electronic mail. The Data Protection Authority can identify other appropriate systems according to new advances in technology. When it refers to exercising the rights referred to under Section 7, paragraphs 1 and 2, the request can also be made verbally, and in this case is noted in summary by the person in charge of the processing or the Data processor.

2. In exercising the rights referred to under Section 7, the data subject can issue a mandate or letter of attorney in writing to natural persons, institutions, associations or entities. The data subject may also be assisted by someone in their trust.

3. The rights under Section 7 referring to personal data pertinent to the deceased may be exercised by whoever has a personal interest, or acts to protect the data subject or for family reasons requiring protection.

4. The data subject's identify is verified according to appropriate assessment criteria, and using the available or submitted deeds and documents, or attached copies of an ID document. The person acting on behalf of the data subject must present or attach a copy of the letter of attorney, or mandate signed in the presence of a person in charge of the processing or signed and submitted together with an unauthenticated photostat copy of the data subject's ID document. If the data subject is a legal person, entity or association, the request is made by the natural person authorised to do so by the respective Articles of Association or regulations.

5. Requests pertinent to Section 7, paragraphs 1 and 2 are freely formulated without any constraints, and may be resubmitted at an interval of not less than ninety days, unless there are substantiated grounds to do so.

8.4 Response to the data subject

1. To ensure that the rights referred to under Section 7 can effectively be exercised, the Data Controller is obliged to adopt appropriate measures aimed especially at:

   a. facilitating the data subject's access to personal data, including the use of appropriate computer software focusing on an accurate selection of data referring to an individual identified or identifiable data subject;
   b. simplifying the procedures and reducing the response time in respect of the requesting party, even with offices or services dedicated to public relations.

2. The data can be extracted by the Data processor or persons in charge of the processing, and can be communicated verbally to the requesting party, or viewed using electronic means; on condition that it is easy to understand the data, and in terms of the quality and quantity of data. If so required, the data can be transposed to hard-copy or electronic formats, or forwarded electronically.

3. Unless the request refers to specific processing or specific personal data or categories of personal data, the response to the data subject includes all the personal data relevant to the data subject, however this may be processed by the Data Controller. If the request is directed to a health professional or health authority, the provisions under Section 84,

paragraph 1 will apply.

4. When the data extraction is especially difficult, the response to the data subject's request can also be done by displaying or delivering copies of the deeds and documents containing the requested personal data.

5. The right to receive the communication with data in an intelligible format does not refer to personal data related to third parties, unless the breakdown of the data processed or the removal of certain elements makes the data subject's personal data incomprehensible.

6. The communication of data must be done in an intelligible format, even in an understandable handwritten format. In the case of communications relating to codes or acronyms, the necessary parameters are provided by the persons in charge of the processing so as to under the relevant meaning.

7. When a request is received pursuant to Section 7, paragraphs 1 and 2, points a), b) and c), and there is no confirmation that data relating to the data subject exists, a contribution may be required, which does not exceed the costs effectively incurred for the search in the specific case.

8. The contribution under Section 7 cannot nonetheless exceed the amount set by the Data Protection Authority under its generally applicable provisions, which can be set at a flat-rate in respect of cases where the data is processed using electronic means and the response is provided verbally. With the same directive, the Data Protection Authority can establish that a contribution may be requested when the personal data is found on a special support that requires a copy to be made thereof, or when significant resources need to be involved with one or more Data Controllers in respect of the complexity or the extent of the requests, and there is confirmation that data exists relating to the data subject.

9. The contribution referred to under paragraphs 7 and 8 is paid by postal or bank crediting of accounts, or by credit or debit card, where possible on receipt of the response and not later than fifteen days from said response.

PART II

Table 1.1 – List of structures where processing is done

Structure: REBYU SRL				
Registered office	Address		City	
Rome	Via Lima, 7		Rome (RM)	
Type of access	Access to the public	Alarm	Closing	Fire prevention system
Controlled with intercom system	Allowed but no clients received	no	Lock	4 fire extinguishers

Reference structure: details the structure (office, function, etc..) where the processing is done. In the case of complex structures, details are provided on the macro-structure (management, department or staff service), or the specific offices within the above (contracts office, human resources, trade union disputes, administration-accounting).

Premises: place where the institution, entity, office, organisation and similar are located and where the data processing is done. Specify any head offices and secondary offices where the personal data is effectively processed.

It is noted that the office premises where the processing is done is accessible through the main entrance accessible to the public, but that is no reception for the public.

Access to secured areas

At the entrance of the office there is a workstation uses as a reception. The person in charge responsible for the reception checks office accesses.
HR department send a list of active employee at the beginning of the year and every time occur a change to permit receptionist checking the active people.
Every active people with a subscribed regular contract can enter into their workstation area.
In case of dismissed employee wants come in, he will be identified through the same procedure of one day visitor [see next point] and carry during the period dedicated to the visit.

Daily HR department send a list that includes all the scheduled visits, all the interview and all the training session with the participants' details.
Each visitor (included sales agents) is identified and registered proving their ID document.
After the identification the receptionist give them a paper badge that allowed a temporary access for the time strictly necessary to the scheduled visit.
The badge not allow the opening of any entrance because it isn't an electronic device.

Visitors are signed into the building by an employee, they are issued numbered visitor badges, required to be turned in at the end of the day.
Special precautions are required for deeds, documents and supports containing sensitive and judicial data: persons in charge of the processing in this case are required to put in place controls and safeguard the data so that it is not accessible to unauthorised persons. In this regard, persons in charge of the processing have a place set up as an archive that can be locked, where they must place documents containing sensitive or judicial data, before leaving their workplace, even if this is temporarily. Documents can also be placed here at the end of the working day, should the person in charge of the processing need to continue using them the following day.
Once processing is completed, the person in charge of the processing must then place the deeds, documents and supports that are no longer necessary to conduct their work.
With regard to filing, the Data Controller has specific areas, where documents, deeds and supports containing personal data are kept in an ordered fashion, and separated according to the different Company functions.
Special precautions are required for the filing of documents, deeds and supports containing sensitive and judicial data: these are stored in places, cupboards or similar devices that can be locked.

After working hours, the key to the archive is given to the Data Controller.

Table 1.2 – List of databases subject to processing

NAME OF DATABASE no. 1 – DOCUMENTS	
Description	XLS, DOC, PDF FILES
Type of database	FOLDERS OF FILES
Type of data	COMMON AND SENSITIVE DATA
Relevant categories	CUSTOMERS AND SUPPLIERS
Data processor	MAURIZIO DI DOMENICO
Purpose	ADMINISTRATIVE MANAGEMENT
Type of processing	ELECTRONIC MEANS AND HARD-COPY
Notes	
PROCESSING SYSTEM	
Processing system	Personal computer
Type of support	Hard disk
Access data to the system	Access to the archive with password Six-monthly password change Impossible to independently change password Concurrent access with same authorisation credential not allowed Annual check on authorisation profile
Reference structure	REBYU SRL
Registered office	VIA LIMA 7 - 00162 ROMA

NAME OF DATABASE no. 2 – DOCUMENTS		
Description	XLS, DOC, PDF FILES	
Type of database	FOLDERS OF FILES	
Type of data	COMMON AND SENSITIVE DATA	
Relevant categories	CUSTOMERS AND SUPPLIERS	
CEO		
Purpose	ADMINISTRATIVE MANAGEMENT	
Type of processing	ELECTRONIC MEANS AND HARD-COPY	
Notes		
PROCESSING SYSTEM		
Processing system	Personal computer	
Type of support	Hard disk	
Access data to the system	Access to the archive with password Six-monthly password change Impossible to independently change password Concurrent access with same authorisation credential not allowed Annual check on authorisation profile	
Reference structure	REBYU SRL	
Registered office	VIA LIMA, 7 - 00100 ROMA	

NAME OF DATABASE no. 3 – DOCUMENTS	
Description	XLS, DOC, PDF FILES
Type of database	FOLDERS OF FILES
Type of data	COMMON AND SENSITIVE DATA
Relevant categories	CUSTOMERS AND SUPPLIERS
Data processor	
Purpose	ADMINISTRATIVE MANAGEMENT
Type of processing	ELECTRONIC MEANS AND HARD-COPY
Notes	

PROCESSING SYSTEM	
Processing system	Personal computer
Type of support	Hard disk
Access data to the system	Access to the archive with password Six-monthly password change Impossible to independently change password Concurrent access with same authorisation credential not allowed Annual check on authorisation profile
Reference structure	REBYU SRL
Registered office	VIA LIMA, 7 - 00100 ROMA

NAME OF DATABASE no. 4 – DOCUMENTS	
Description	XLS, DOC, PDF FILES
Type of database	FOLDERS OF FILES
Type of data	COMMON AND SENSITIVE DATA
Relevant categories	CUSTOMERS AND SUPPLIERS
Data processor	
Purpose	ADMINISTRATIVE MANAGEMENT
Type of processing	ELECTRONIC MEANS AND HARD-COPY

Notes		
PROCESSING SYSTEM		
Processing system	Personal computer	
Type of support	Hard disk	
Access data to the system	Access to the archive with password Six-monthly password change Impossible to independently change password Concurrent access with same authorisation credential not allowed Annual check on authorisation profile	
Reference structure	REBYU SRL	
Registered office	VIA LIMA, 7 - 00100 ROMA	

NAME OF DATABASE no. 5 – DOCUMENTS		
Description	XLS, DOC, PDF FILES	
Type of database	FOLDERS OF FILES	
Type of data	COMMON AND SENSITIVE DATA	
Relevant categories	CUSTOMERS AND SUPPLIERS	
CEO		
Purpose	ADMINISTRATIVE MANAGEMENT	
Type of processing	ELECTRONIC MEANS AND HARD-COPY	
Notes		
PROCESSING SYSTEM		
Processing system	Personal computer	
Type of support	Hard disk	
Access data to the system	Access to the archive with password Six-monthly password change Impossible to independently change password Concurrent access with same authorisation credential not allowed Annual check on authorisation profile	
Reference structure	REBYU SRL	
Registered office	VIA LIMA, 7 - 00100 ROMA	

NAME OF DATABASE no. 6 – DOCUMENTS		
Description	XLS, DOC, PDF FILES	
Type of database	FOLDERS OF FILES	
Type of data	COMMON AND SENSITIVE DATA	
Relevant categories	CUSTOMERS AND SUPPLIERS	
CEO		
Purpose	ADMINISTRATIVE MANAGEMENT	
Type of processing	ELECTRONIC MEANS AND HARD-COPY	
Notes		
PROCESSING SYSTEM		
Processing system	Personal computer	
Type of support	Hard disk	
Access data to the system	Access to the archive with password Six-monthly password change Impossible to independently change password Concurrent access with same authorisation credential not allowed Annual check on authorisation profile	
Reference structure	REBYU SRL	
Registered office	VIA LIMA, 7 - 00100 ROMA	

NAME OF DATABASE no. 7 – DOCUMENTS	
Description	XLS, DOC, PDF FILES
Type of database	FOLDERS OF FILES
Type of data	COMMON AND SENSITIVE DATA
Relevant categories	CUSTOMERS AND SUPPLIERS
CEO	
Purpose	ADMINISTRATIVE MANAGEMENT
Type of processing	ELECTRONIC MEANS AND HARD-COPY
Notes	
PROCESSING SYSTEM	
Processing system	Personal computer
Type of support	Hard disk
Access data to the system	Access to the archive with password Six-monthly password change Impossible to independently change password Concurrent access with same authorisation credential not allowed Annual check on authorisation profile
Reference structure	REBYU SRL
Registered office	VIA LIMA, 7 - 00100 ROMA

NAME OF DATABASE no. 8 – DOCUMENTS	
Description	XLS, DOC, PDF FILES
Type of database	FOLDERS OF FILES
Type of data	COMMON AND SENSITIVE DATA
Relevant categories	CUSTOMERS AND SUPPLIERS
CEO	
Purpose	ADMINISTRATIVE MANAGEMENT
Type of processing	ELECTRONIC MEANS AND HARD-COPY
Notes	
PROCESSING SYSTEM	
Processing system	Personal computer
Type of support	Hard disk
Access data to the system	Access to the archive with password Six-monthly password change Impossible to independently change password Concurrent access with same authorisation credential not allowed Annual check on authorisation profile
Reference structure	REBYU SRL
Registered office	VIA ARDUINO 22 - 00162 ROMA

NAME OF DATABASE no. 9 – DOCUMENTS	
Description	XLS, DOC, PDF FILES
Type of database	FOLDERS OF FILES
Type of data	COMMON AND SENSITIVE DATA
Relevant categories	CUSTOMERS AND SUPPLIERS
CEO	
Purpose	ADMINISTRATIVE MANAGEMENT
Type of processing	ELECTRONIC MEANS AND HARD-COPY
Notes	
PROCESSING SYSTEM	
Processing system	Personal computer

Type of support	Hard disk	
Access data to the system	Access to the archive with password Six-monthly password change Impossible to independently change password Concurrent access with same authorisation credential not allowed Annual check on authorisation profile	
Reference structure	REBYU SRL	
Registered office	VIA LIMA, 7 - 00100 ROMA	

Name of database: List of databases managed by the Data Controller;
Description: Contains the descriptions of each specific database;
Relevant categories: contains the list of all categories of data subjects involved in the processing of data (e.g. employees, customers, associates, etc…), in respect of the different databases;
Purposes: list of purposes that the personal data contained in the databases managed by the Data Controller are processed for and the relevant structures;
Access data to the system: lists the types of data processed that are contained in various databases defined by the user; these can be classified as:

- COMMON DATA, namely the class of data at less risk, where specific security measures are not required;
- SENSITIVE/JUDICIAL PERSONAL DATA, namely the class of data at high risk.

Reference structure: Specifies the structure where the database is kept and managed in the order of the listing;
Registered office: Location where the above mentioned structure is found.

Table 1.3 – List of names per structure

Data Controller - REBYU SRL				
VAT NO.	Address	City	Tel./Fax/e-mail	Category
13656681007	Via LIMA, 7	Roma	0645555216 0645555217	Limited liability company (private entity)

Name of internal entities responsible for data processing - Structure: REBYU SRL

Persons in charge of the processing		
Name and surname	Profile	E-mail
TBD	Admin Employee	
TBD	BO Employee	
TBD	HR Employee	
TBD	HR Employee	
TBD	BO Employee	
TBD	BO Employee	
TBD	BO Employee	
TBD	BO Employee	
TBD	BO Employee	

Classification of data processed: the data in a database can be subdivided as follows:

- PERSONAL DATA
- COMMON DATA, namely the class of data at less risk, where specific security measures are not required;
- PERSONAL SENSITIVE/JUDICIAL DATA, namely the class of data at high risk

Name of external entities responsible for data processing - Structure: REBYU SRL

Data Controller:			
Address	City	Tel./Fax/e-mail	Category
tbd			

Data Controller: GPD - - studio legale e tributario			
Address	City	Tel./Fax/e-mail	Category
tbd			

Data Controller:			
Address	City	Tel./Fax/e-mail	Category
tbd			

Table 1.4 List of entities authorised for data processing

Processing done by REBYU SRL
Description of structure's tasks and responsibilities
Vehicle for American Express products on PS channel, via a number agent spread over the Country

Name of database	Description of database	Person in charge of processing
NO. 1 DOCUMENTS	XLS, DOC, PDF FILES	
NO. 2 DOCUMENTS	XLS, DOC, PDF FILES	
NO. 3 DOCUMENTS	XLS, DOC, PDF FILES	
NO. 4 DOCUMENTS	XLS, DOC, PDF FILES	
NO. 5 DOCUMENTS	XLS, DOC, PDF FILES	
NO. 6 DOCUMENTS	XLS, DOC, PDF FILES	
NO. 7 DOCUMENTS	XLS, DOC, PDF FILES	
NO. 8 DOCUMENTS	XLS, DOC, PDF FILES	
NO. 9 DOCUMENTS	XLS, DOC, PDF FILES	

Processing done by the structure: list of purposes that the personal data contained in the databases managed by the Data Controller are processed for and the relevant structures;

__**Description of structure's tasks and responsibilities**__: Specify the methods used for processing the data contained in the relevant database.

The Data processor for the personal data is responsible for:

- appointing the persons in charge of the processing for the databases that have been entrusted to him/her;
- monitoring that the processing is done within the deadlines and the methods set by the Personal Data Protection Code;
- providing adequate instructions to the persons in charge of the processing done using electronic and non-electronic means;
- periodically checking (at least on an annual basis), that the conditions exists to retain the persons in charge of the processing authorisation profile.
- Guaranteeing that all the required personal data security measures have been applied;
- Preparing and updating any change to the list of premises where data is processed;
- Preparing and updating any change to the list of offices where data is processed;
- Preparing and updating any change to the list of databases subject to processing;
- preparing and updating any change to the list of processing systems, if the processing is done using electronic means;
- Defining and subsequently periodically checking the access arrangements (on at least a six-monthly basis) to the premises and the measures adopted to protect the spaces and premises, which are relevant in terms of their custody and accessibility, as specified below;
- Deciding whether to entrust the entire or part of the data processing to structures outside the Data Controller;
- Should the data processing be entrusted to structures outside the Data Controller, checking and guaranteeing that all security measures referring to personal data have been applied;
- If the processing is done using electronic means, identifying, nominating and appointing in writing one or more persons in charge of managing and maintaining the electronic devices;
- If the processing is done using electronic means, identifying, nominating and appointing in writing one or more persons in charge of keeping the copies of the credentials in the case of there being more than one person in charge of the processing;
- If the processing is done using electronic means, identifying, nominating and appointing in writing one or more persons in charge of the databases' back-up copies;
- Keeping and retaining the supports used for the data back-ups;
- In respect of the work conducted, the Person in charge of the personal data security must if deemed necessary, identify, nominate and appoint in writing, one or more Persons in charge of specific processing with the task of identifying, nominating and appointing in writing the persons in charge of the processing of personal data;
- If the Person in charge of personal data security does not appoint a Data processor, the former will take on all the relevant responsibilities and functions.

The personal data processing is only carried out by entities that have been formally appointed; this is done by the documented assigning of each person to a unit, where the processing context that is permitted to those in the unit has been identified in writing beforehand.
In addition to general instructions on how to process the personal data, the persons in charge of the processing are provided with explicit instructions on the following points referring to security:

- the procedures to follow for the classification of data, so as to distinguish sensitive and judicial data, to guarantee the security of data requiring higher precaution levels, compared to the requirements for common data,

- the methods for processing documents containing personal data, and the methods to comply with for retaining and filing data, once the work that the documents were required for has been completed,
- the methods for processing and safeguarding passwords needed to access electronic computers and the data they contain, as well as providing a copy f this to the Person in charge of safeguarding passwords,
- directive not to leave electronic means unattended and accessible, while a work session is in progress, by way of:
- Screen-savers with passwords
- procedures and arrangements for using the tools and programmes aimed at protecting information systems
- procedures for saving data
- arrangements for safekeeping and use of removable supports, containing personal data
- obligation to keep updated, using the material and tools provided by the Data Controller on security measures.

The persons in charge of the management and maintenance of information systems, whether internal or external to the Data Controller's organisation, are not permitted to carry out any processing on personal data contained in the electronic means, with the exception of temporary processing that is strictly necessary to carry out system management and maintenance.

The letters and contracts appointing data processors, the letters of designation for persons in charge of the processing are collected in an orderly fashion, based on the organisational unit the entities belong to: in this way, the Data processor has a clear picture of who is doing what (privacy function) in the context of processing personal data. On a periodic basis at least once a year, the data that the persons in charge of the processing are authorised to access is updated, together with the processing they are authorised to put in place, in order to verify that the conditions justifying said authorisations still exist. The same operation is carried out in respect of authorisations issued to persons in charge of managing and maintaining electronic means.

Table 2 - Risks analysis

The table below details the events that could potentially cause damage to all or part of the resources needed to retain the data subject to processing. The risks are classified in relation to the event that brings them about, they are consequently determined by:

- Operator behaviour;
- Events relative to tools;
- Events relative to context.

Name of database: N. 1-2-3-4-5-6-7-8-9 DOCUMENTS	**Structure: REBYU SRL**
Risks	Description of impact on security (Level of Risk: Very low/Low/Medium/High)
Data loss	low

Operator behaviour	
Risk	Risk assessment
Loss of data due to incorrect shutdown of personal computer	low

Events relative to tools	
Tool events risk	Tool events risk assessment
Fire	Low
Events relative to context	
Context events risk	Context events risk assessment
Natural events (earthquake)	Low

Risks: list of risks for each database and the relative structure where processing takes place;
Description of impact on security: Impact on security, result of the sum between frequency and magnitude.

ANNUAL HARDWARE RISKS REPORT

Name of processing system	Personal Computer no. 01
Model	Assembled PC
Brand	Intel
Operating system	64 bit -Windows 10
Person in charge of processing	
System administrator	

Name of processing system	Personal Computer no. 02
Model	Assembled PC
Brand	Intel
Operating system	64 bit -Windows 10
Person in charge of processing	
System administrator	

Name of processing system	Personal Computer no. 03
Model	HP
Brand	Intel
Operating system	64 bit -Windows 10
Person in charge of processing	
System administrator	

Name of processing system	Personal Computer no. 04
Model	DELL
Brand	Intel
Operating system	64 bit -Windows 10
Person in charge of processing	
System administrator	

Name of processing system	Personal Computer no. 05
Model	Assembled PC
Brand	Intel
Operating system	64 bit -Windows 7
Person in charge of processing	
System administrator	

Name of processing system	Personal Computer no. 06
Model	HP
Brand	AMD
Operating system	64 bit - Windows 8
Person in charge of processing	
System administrator	

Name of processing system	Personal Computer no. 07
Model	Assembled PC
Brand	Intel
Operating system	64 bit - Windows 10
Person in charge of processing	
System administrator	

Name of processing system	Personal Computer no. 08
Model	DELL
Brand	Intel
Operating system	64 bit -Windows 10
Person in charge of processing	
System administrator	

Name of processing system	Personal Computer no. 09
Model	Assembled PC
Brand	AMD
Operating system	32 bit -Windows 7
Person in charge of processing	
System administrator	

ANNUAL SOFTWARE RISKS REPORT

SOFTWARE	64 bit -Windows 10		
VERSION			
Processing system no. 1 with installation of	Intel Assembled PC		
Assessment date	**Type of risk**	**Risk level**	**Corrective measures**
30/01/2021	DATA LOSS	Low	WEEKLY BACK-UP

SOFTWARE	64 bit -Windows 10		
VERSION			
Processing system no. 2 with installation of	Assembled PC Intel		
Assessment date	**Type of risk**	**Risk level**	**Corrective measures**
30/01/2022	DATA LOSS	Low	WEEKLY BACK-UP

SOFTWARE	64 bit -Windows 10		
VERSION			
Processing system no. 3 with installation of	HP Intel		
Assessment date	**Type of risk**	**Risk level**	**Corrective measures**
30/01/2021	DATA LOSS	Low	WEEKLY BACK-UP

SOFTWARE	64 bit -Windows 10		
VERSION			
Processing system no. 4 with installation of	DELL Intel		
Assessment date	**Type of risk**	**Risk level**	**Corrective measures**
30/01/2021	DATA LOSS	Low	WEEKLY BACK-UP

SOFTWARE	64 bit -Windows 7		
VERSION			
Processing system no. 5 with installation of	Assembled PC Intel		
Assessment date	**Type of risk**	**Risk level**	**Corrective measures**
30/01/2021	DATA LOSS	Low	WEEKLY BACK-UP

SOFTWARE	64 bit - Windows 8		
VERSION			
Processing system no. 6 with installation of	HP AMD		
Assessment date	**Type of risk**	**Risk level**	**Corrective measures**
30/01/2021	DATA LOSS	Low	WEEKLY BACK-UP

<table>
<tr><td colspan="2"><b>SOFTWARE</b></td><td colspan="3">64 bit - Windows 10</td></tr>
<tr><td colspan="2"><b>VERSION</b></td><td colspan="3"></td></tr>
<tr><td colspan="2"><b>Processing system no. 7 with installation of</b></td><td colspan="3">Assembled PC Intel</td></tr>
<tr><td><b>Assessment date</b></td><td colspan="2"><b>Type of risk</b></td><td><b>Risk level</b></td><td><b>Corrective measures</b></td></tr>
<tr><td>30/01/2021</td><td colspan="2">DATA LOSS</td><td>Low</td><td>WEEKLY BACK-UP</td></tr>
</table>

<table>
<tr><td colspan="2"><b>SOFTWARE</b></td><td colspan="3">64 bit -Windows 10</td></tr>
<tr><td colspan="2"><b>VERSION</b></td><td colspan="3"></td></tr>
<tr><td colspan="2"><b>Processing system no. 8 with installation of</b></td><td colspan="3">DELL Intel</td></tr>
<tr><td><b>Assessment date</b></td><td colspan="2"><b>Type of risk</b></td><td><b>Risk level</b></td><td><b>Corrective measures</b></td></tr>
<tr><td>30/01/2021</td><td colspan="2">DATA LOSS</td><td>Low</td><td>WEEKLY BACK-UP</td></tr>
</table>

<table>
<tr><td colspan="2"><b>SOFTWARE</b></td><td colspan="3">32 bit -Windows 7</td></tr>
<tr><td colspan="2"><b>VERSION</b></td><td colspan="3"></td></tr>
<tr><td colspan="2"><b>Processing system no. 9 with installation of</b></td><td colspan="3">Assembled PC AMD</td></tr>
<tr><td><b>Assessment date</b></td><td colspan="2"><b>Type of risk</b></td><td><b>Risk level</b></td><td><b>Corrective measures</b></td></tr>
<tr><td>30/01/2021</td><td colspan="2">DATA LOSS</td><td>Low</td><td>WEEKLY BACK-UP</td></tr>
</table>

In the future, the updating of these programmes will be done at least on an annual basis, and on a six-monthly basis in respect of the tools that process sensitive or judicial data. Updates will be done manually for programmes without these functions.

Rome, 07/06/2024

Table 3 – Criteria and procedures for restoring data availability

RESTORE - Name of database: N. 1-2-3-4-5-6-7-8-9 DOCUMENTS Structure: REBYU SRL	
Criteria and procedures for restoring data	Planning of restoring tests
Recovery through back-up	Restoring intervals: Yearly

SAVING - Name of Database:	
Criteria and procedures for saving data	*Place copies are kept*
Type of Support: hard disk Back-up frequency: Weekly	REBYU SRL

Criteria and procedures for restoring data: Procedure followed for restoring the specific database;
Planning of restoring tests: Details of the plan to put in place in the event of restoring a specific database containing the data being processed;
Criteria and procedures for saving data: Procedure followed to Back-up a specific database;
Place copies are kept: Place where the Back-up copies of a specific database are kept.

Table 4 – Planning of required training sessions

Structure: REBYU SRL		
Summarised description of training sessions	Relevant person in charge of the processing	Time requirement

Legislative decree no. 196 of 30 June 2003 - Personal Data Protection Code.	HIDEEA SRL	h. 1

Summarised description of training sessions: Subject of the training provided to the person in charge of the processing that processes data in a database and/or manages the latter;
Relevant person in charge of processing: Person in charge of the processing undergoing training;
Time requirement: The time to provide the training.

The importance of training members of the team is recognised in respect of security, constituting a significant aspect in reducing risks to the system and there is an undertaking to encourage training, especially from the time of the designation, or when someone changes functions, or new electronic tools are introduced that impact on the processing of personal data. All members of individual companies must in any case participate once a year in refresher courses, aimed at ensuring they are duly informed on the following aspects:

- the regulations on the protection of personal data, which are most relevant for the persons in charge of the processing's work, and the resulting responsibilities
- risks incumbent to data
- measures available to prevent damaging events
- Arrangement for updating security measures.

The training sessions are scheduled once a year to take place or when one of the following circumstances arises:

- at the time of a new designation within 30 days from the start
- when there is a change in function that implies significant changes in respect of the processing of personal data
- When new important tools are introduced, which imply significant changes in the processing of personal data.

Security Awareness Program Checklist

- Awareness of phone, mail, fax
- Importance of strong passwords and password controls
- Secure e-mail practices
- Avoiding malicious software – viruses, spyware, adware, etc.
- Secure browsing practices

Creating the Security Awareness Program

- Identify compliance or audit standards that your organization must adhere to.
- Identify security awareness requirements for those standards.
- Identify organizational goals, risks, and security policy.
- Identify stakeholders and get their support.
- Create a baseline of the organization’s security awareness.
- Create project charter to establish scope for the security awareness training program.
- Create steering committee to assist in planning, executing and maintaining the awareness program.
- Identify who you will be targeting—different roles may require different/additional training (employees, IT personnel, developers, senior leadership).
- Identify what you will communicate to the different groups (goal is shortest training possible that has the greatest impact).
- Identify how you will communicate the content—three categories of training: new, annual, and ongoing.

Implementing Security Awareness

- Develop and/or purchase training materials and content to meet requirements identified during program creation.
- Document how and when you intend to measure the success of the program.
- Identify who to communicate results to, when, and how.
- Deploy security awareness training utilizing different communication methods identified during program creation.
- Implement tracking mechanisms to record who completes the training and when.

Sustaining Security Awareness

- Identify when to review your security awareness program each year.

- Identify new or changing threats or compliance standards and updates needed; include in annual update.
- Conduct periodic assessments of organization security awareness and compare to baseline.
- Survey staff for feedback (usefulness, effectiveness, ease of understanding, ease of implementation, recommended changes, accessibility).
- Maintain management commitment to supporting, endorsing and promoting the programme.

Rome 01/05/2024

Table 4.1 – Training plan for persons in charge of back-up

Database	Name and Surname	Need to provide training	Training plan/Courses
DATA		NONE	

All personal data managed by electronic means in the Company is included in the back-up procedure. Back-up is done weekly and usually on a Saturday. Back-up supports are titled and stored using labels. The most recent back-up copies are placed in a: STORAGE BOX. The penultimate data back-up copies are kept in places other than the individual Company and more specifically in binders. The time needed to recover data from the back-up copies when there is a general emergency is estimated to be a few hours from the time the possible negative event occurs. This is well below the limit of the seven days required by point 23 of Annex B to Legislative Decree 196/2003 in the case of processing sensitive data.

The recovery is done using an appropriate manager programme provided to the unit responsible for backing-up. The Disaster Recovery Manager and the keeper of the back-up supports is the Company's Data Controller.

The Person in charge of backing-up databases is responsible for:

Taking all the necessary measures to avoid the loss or destruction of data, and arrange for the periodic recovery of these with back-up copies, according to the criteria set by the Person in charge of personal data security;

Ensuring the quality of the data back-up copies and that they are kept in a suitable and safe place; Ensuring the data back-up copies are kept in a suitable and safe place with controlled access; Arrange to carefully keep the devices used to make the back-ups, preventing unauthorised staff from gaining access;

Promptly advise the Person in charge of managing and maintaining electronic means of any problems that could arise during the normal back-up operations; The persons in charge of database back-up declares that they are cognisant of the tasks entrusted to them, and to be aware of the provisions under the Personal Data Protection Code and undertake to adopt all necessary measures to implement the provisions of the Code.

The label attached to each support must contain the following information: Date when Back-up copy was made

Back-up instructions	Check there are no connections

Back-up verification instructions	
Back-up recovery instructions	

Rome, 07/06/2024

Table 5 – Assigning processing

Name of database: N. 1-2-3-4-5-6-7-8-9 DOCUMENTS Structure: REBYU SRL
Internal data processor
CEO
Purpose of the activity
ADMINISTRATIVE MANAGEMENT
Arrangements for relevant data
ELECTRONIC MEANS AND HARD-COPY

Purpose of the outsourced activity: List of purposes for processing databases managed by entities outside the structure;
Arrangements for relevant data: Processing methods for data carried out by entity outside the reference structure;

In respect of entities carrying out the entirety or partial data processing outside the Data Controller's structure, the data processors of personal data are appointed outside the Data controller's structure (outsourcing), pursuant to Sec. 28 of the Personal Data Protection Code. The latter are to be considered independent Data Controllers and therefore subject to the relevant obligations, and are consequently directly and solely liable for any breach of the law.
The Data processor for outsourced data declares that he/she is aware of the provisions under the PDP Code regarding personal data, and the technical specifications on minimum security measures, and undertakes to adopt all the measures needed to implement the provisions therein and specifically those referred to under Sec. 11, paragraphs 1 and 2.
The Data processor for outsourced data declares further that once the processing is completed, he/she undertakes to return all the information constituting the database being processed to the Data Controller, and that all the copies of the data in whatever format (hard-copy, magnetic, etc.) will be cancelled or destroyed.
The Data processor for outsourced data undertakes not to communicate the data entrusted to any third parties, without prior authorisation from the Data Controller.

Rome, 07/06/2024

Table 6 – Processing systems for the processing of data

A list of the processing system located in a specific structure and where the database is found, which are subject to data processing.

Name of database: NO. 1 DOCUMENTS - Structure: REBYU SRL	
Model	Assembled PC
Brand	Intel
Operating system	64 bit -Windows 10
Person in charge of processing	
Type of connection	COMPANY NETWORK AND INTERNET
Antivirus	AVIRA CONNECT
System data processor	
System administrator/maintenance	DBNET S.R.L.
Password custodian	
List of Supports	
Processing supports: INTERNAL HARD DISK – DVD DISC DRIVE	
List of Software	
Processing software: OFFICE BUSINESS 2010	

Name of database: NO. 2 DOCUMENTS - Structure: REBYU SRL	
Model	Assembled PC
Brand	Intel
Operating system	64 bit -Windows 10
Person in charge of processing	
Type of connection	COMPANY NETWORK AND INTERNET
Antivirus	AVIRA CONNECT
System data processor	
System administrator/maintenance	DBNET S.R.L.
Password custodian	
List of Supports	
Processing supports: INTERNAL HARD DISK – DVD DISC DRIVE	
List of Software	
Processing software: OFFICE BUSINESS 2010	

Name of database: NO. 3 DOCUMENTS - Structure: REBYU SRL	
Model	HP
Brand	Intel
Operating system	64 bit -Windows 10
Person in charge of processing	
Type of connection	COMPANY NETWORK AND INTERNET

Antivirus	AVIRA CONNECT
System data processor	
System administrator/maintenance	DBNET S.R.L.
Password custodian	
List of Supports	
Processing supports: INTERNAL HARD DISK – DVD DISC DRIVE	
List of Software	
Processing software: OFFICE BUSINESS 2010	

Name of database: NO. 4 DOCUMENTS - Structure: REBYU SRL	
Model	DELL
Brand	Intel
Operating system	64 bit -Windows 10
Person in charge of processing	
Type of connection	COMPANY NETWORK AND INTERNET
Antivirus	AVIRA CONNECT
System data processor	
System administrator/maintenance	DBNET S.R.L.
Password custodian	
List of Supports	
Processing supports: INTERNAL HARD DISK – DVD DISC DRIVE	
List of Software	
Processing software: OFFICE BUSINESS 2010	

System administrator: the entity tasked with overseeing the resources of the computer's operating system or data base system and allows the use thereof. In this context, the system administrator also assumes the functions of network administrator, namely the entity that oversees the network resources and allows the use thereof.

For security reasons, the system administrator covers the responsibilities set out in the letter of designation.

Person in charge of maintenance: the entity appointed by the Data Controller or Data processor, with the task of maintaining the system holding the database subject to processing. With specific reference to security, the person in charge of maintenance covers the responsibilities set out in the letter of designation.

<u>Password custodian:</u> the entity entrusted with the management of passwords are the persons in charge of the processing in accordance with the tasks detailed in the letter of designation.

<u>List of Supports:</u> List of supports where the database physically reside.

<u>List of Software:</u> List of software found on the machine where the specific database exists.

The person in charge of managing and maintaining electronic means is responsible for:

- Activating the authentication credentials for persons in charge of the processing, on the orders of the Data processor, for all processing done by electronic means;
- Protecting the computers from the risk of intrusions (hackers violating the system);
- Notifying the Data Processor should risks be found relating to the security measures referring to personal data.

Loss of data due to flooding

With regard to the risk of data being lost due to flooding, and considering the building's position, this risk is excluded, unless there are totally unforeseen and exceptional events.

In any event, the computer equipment has been raised off the ground.

Loss of data due to fire

With regard to the risk of data being lost due to fire, it is noted that the measures required by current legislation have been implemented in respect of fire prevention, including periodic checking of electrical installations.

REBYU Srl has activated an authentication system that is currently operational for each person in charge of processing personal data:

- this is associated with an ID code for the person in charge of the processing (username), attributed by whoever administers the system, a confidential password, known only to the person in charge of processing, who is responsible for its processing, keeping it confidential and changing it periodically.

Persons in charge of the processing are notified that the password cannot be less than eight characters in length, unless there are technical limitations in the software being used.

The persons in charge of the processing must take certain measures in processing the password:

- they must contain references that cannot easily be associated with the data subject (not only names, surnames, nicknames, but also one's date of birth, children's or friends' dates of birth), or consist of well-known names, even cartoon characters (Goofy, Pluto, Donald Duck).
- A general rule is for a quarter of the characters making up the password to be numbers.

Passwords must not be communicated to anyone (not only external entities, but also people belonging to the organisation, whether colleagues, data processors, system administrators or data controllers).

The person in charge of the processing is advised to change their password at least every 6 months.

In the event of sensitive data, the person in charge of the processing is advised to change their password at least every 3 months.

Authentication credentials are deactivated in the case of one of the following:

- Immediately, if the person in charge of the processing loses the quality that allowed access to the tool
- in any case, within six months of not being used.

The identification and authentication systems also operate on portable computers that manage and contain personal data.

Our organisation decided to extend these rules to any kind of support containing personal data, even common data, and imposing the following on persons in charge of the processing:

- Supports must be kept and used in such a way that prevents unauthorised access (theft included) and processing that is not allowed: in particular, they must be kept in locked drawers while being used, and then formatted, when the purpose that the data stored on them for has lapsed.

Once the reason for keeping the date no longer exists, the necessary measures must be taken to render the data contained on the supports unintelligible and incapable of being reconstructed technically. This must then be cancelled if possible, and the supports also cancelled if necessary.

As far as the loss or damage of data due to a virus is concerned, it is noted that:

- the SYMANTEC ENDPOINT SMALL BUSINESS antivirus is available on the processing systems. This antivirus automatically checks any files deleted from the internet or electronic mail, or read by external supports such as floppy disks or CD-roms.

Updating for new viruses on personal computers is done automatically on a daily basis, and was installed on 19/07/2011.

Rome, 02/05/2024

Table 7 – Permits to access data

List of the permits assigned to al entities that are involved in the processing of personal data for a specific database managed by a structure.

Name of database: No. 1-2-3-4-5-6-7-8-9 Documents - Structure: REBYU SRL				
Entity	Permits			
	Reading	Printing access	Changes	Cancellation
	YES	YES	YES	YES
	YES	YES	YES	YES
	YES	YES	YES	YES
	YES	YES	YES	YES
	YES	YES	YES	YES
	YES	YES	YES	YES
	YES	YES	YES	YES
	YES	YES	YES	YES
	YES	YES	YES	YES

Person in charge of processing: List of all entities involved in the different stages of data processing.

Role: The role that the specific entity covers in the data processing context.

Permits: Permits that the Data Controller or Data processor assign to various entities that work on the data processing of a specific database.

Table 8 – Criteria for assigning access credentials for databases

As the Data processor for databases NO. 1 – 2 – 3 – 4 DOCUMENTS, Mr MAURIZIO DI DOMENICO sets the criteria for assigning access credentials to the following persons in charge of the processing:

_______.

The Person in charge of keeping copies of credentials is responsible for:

- Managing and seeing to the safekeeping of the data access credentials for the persons in charge of the processing;
- For each person in charge of the processing, preparing an envelope containing the name of the person, with the credential used inside the envelope. Envelopes with credentials must be stored in a locked and protected place;
- Instructing the persons in charge of the processing regarding the use of passwords, and the characteristics they should have, as well as the procedures to change them independently;
- Cancelling all unused credentials in the event that person in charge of the processing loses the right to have them;
- Cancelling the access credentials for persons in charge of the processing if they have not been used for over 6 (six) months;
- The person in charge of keeping copies of credentials declares that he/she is cognisant of the tasks entrusted, and to be aware of the provisions under the Personal Data Protection Code and undertakes to adopt all necessary measures to implement the provisions of the Code.

It should be remembered that:

a) access credentials are personal
b) access credentials must not be stored
c) access credentials must not be communicated to anyone
d) access credentials must not be transcribed

Rome, 02/05/2024

Table 9 – Undertaking and signature

This document, prepared on 02/05/2024 is signed at the bottom by: MAURIZIO DI DOMENICO, in his capacity as sole director of the company REBYU Srl; DPO nominated as Antonello Dionisi.
The Data Controller publishes and reviews the ISP once a year.
Every time that it is published and modified the Data Controller communicates to its employees any new or existing security policies on a need to know basis.
At the same time, ISP is published and spread to all contracted field agents who adhere to these information security policies and standards as well.

The original of this document is kept at the Company's offices, and may be presented in the case of inspections.

Rome, 07/06/2024

Signature of Data Controller's representative